# White Papers Volume 3 Book 1




**Air University**
**Maxwell Air Force Base, Alabama**

# WHITE PAPERS

## VOLUME 3, BOOK 1

# POWER AND INFLUENCE

Air University
Maxwell Air Force Base, Alabama

Prepared by
2025 Support Office
Air University
Air Education and Training Command

Developed by
Air University Press
Educational Services Directorate
College of Aerospace Doctrine, Research, and Education
Maxwell Air Force Base, Alabama

November 1996

## Disclaimer

***2025*** is a study designed to comply with a directive from the chief of staff of the Air Force to examine the concepts, capabilities, and technologies the United States will require to remain the dominant air and space force in the future. Presented on 17 June 1996, this report was produced in the Department of Defense school environment of academic freedom and in the interest of advancing concepts related to national defense. The views expressed in this report are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States government.

This report contains fictional representations of future situations/scenarios. Any similarities to real people or events, other than those specifically cited, are unintentional and are for purposes of illustration only.

This publication has been reviewed by security and policy review authorities, is unclassified, and is cleared for public release.

## *Contents*

| *Appendix* | | *Page* |
|---|---|---|
| A | Index of ***2025*** Volumes | 329 |
| B | Project Participants | 335 |

**Illustrations**

*Figure*

***Frontier Missions: Peacespace Dominance***



***Information Operations: A New War-Fighting Capability***



***A Contrarian View of Strategic Aerospace Warfare***



***Interdiction: Shaping Things to Come***

# *Preface*

*Power undirected by high purpose spells calamity; and high purpose by itself is utterly useless if the power to put it into effect is lacking.*

—Theodore Roosevelt

Ultimately, the test of national defense is the ability to apply military force unilaterally in support of the national interest. The array of power at the nation's disposal in support of its interests is crucial to national security. The power that the USAF can employ—both lethal and nonlethal—in the worlds of 2025 is critical to the nation's ability to survive and prosper in a complex, interdependent, constantly changing security environment. That power has many different dimensions—tactical or strategic, conventional or nuclear, command and control or informational, and chemical or biological. The nature of the force available in 2025 will determine the effectiveness of the power of the United States in 2025. Hence, force-structure decisions made now are crucial to the strategic environment of the future.

But power—the application of force, the utilization of military capabilities—is only an instrumental goal. What we really seek is influence—the ability to produce effects on others, directly or indirectly. We want to change an adversary's perceptions, cost-benefit calculations, and action or inaction in accord with our desires. We seek to influence people to make certain choices. The use of power in the application of force is merely one way to do this. Having the power—the force—to compel is a means to deter. We don't use power directly, but we have it, and our possession of certain systems and capabilities may indirectly cause an adversary to change his mind on a course of action. What we seek is not so much global power as global influence. In Douhet's terms, we seek to destroy the enemy's will to resist. That may be done by destroying his capability to resist. But it need not be. All we need do is influence his decision processes.

The papers in this volume investigate numerous systems, technologies, and concepts of operations by which the United States may maintain or increase its technological superiority to leverage asymmetrical advantage in conflict with nearly any adversary to preserve American security in the twenty-first century. Some of these notions may seem rather outlandish and more akin to science fiction than serious military planning. But one must remember that the technology of the future may verge on the incomprehensible. Any speculation about the technology of 2025 that does not seem like magic is probably flawed.

(Please note that appendix A contains a list of all the papers in the ***2025*** study, arranged by volume for ready reference. Also, appendix B contains a list of all the people—military and civilian, warriors and scientists, educators and operators, leaders and supporters—who contributed to the ***2025*** project.)

# Frontier Missions: Peacespace Dominance


Lt Col Thomas F. Baldy
Maj Joseph T. Callahan III
Maj Louise A. Christ
Maj Teresa L. Dicks
Maj Kelvin P. Kearney
Maj Matthew A. Parks
Mr James L. Pullara


## Executive Summary

*Two challenges lie before us: first, to guide, harness, and balance force and diplomacy as we enter the 21st century, and second, to learn how to deal with "operations other than war."*

—Gen John M. Shalikashvili

The word *frontier* evokes an image of such distant borders as the American frontier of the nineteenth century or the beckoning unknown of space. It also suggests austerity, hardship, and lawlessness. The frontier of 2025 will be the streets and fields of the developing world. The battle will be for cooperation of people ravaged by poverty, disease, hunger, and crime. These problems will be epidemic, in some regions driving the US to choose wisely where, when, and how to act. The dilemma of 2025 will mirror today: whether to meet force with force or prevent violence by preempting it.[1] Within a domestic environment of increasing fiscal discipline and regard for life, the most efficient way to defend our national interest is to act before a situation flares into violence.

One possibility is to dampen these violent flare-ups with a force dedicated to preventing or resolving conflict. However, this option requires a profound shift in focus and an unprecedented appreciation of degrees of conflict and hostility. Within each situation, there are instances where the application of lethal military force is appropriate. There are also instances where force is counterproductive. A murky void separates the two.

We need to bridge that void. This paper advocates creating a small, rugged, and specialized composite force dedicated to creating and operating in the physical and psychological state we will call the *peacespace*.[2] The size and composition of the force will be crucial to success or failure. In 30 years, we envision that a composite force will consist of military, civil service, contractor, and international personnel. Aided by technological possibilities and new conceptual thinking, a security assurance force (SAF—pronounced Safe) will foster institutions required for long-term stability in a region.

This stability rests on three core capabilities of SAF: constabulary power (military role), education (civilian role), and infrastructure building (military/civilian). The synergy of these capabilities, harmoniously employed, can dampen or remove violence and attendant fear, allowing a choreographed peace to emerge. SAF will possess sufficient capability to impose order when violence is at a relatively low order of magnitude. If violence is high or escalates, SAF directs standoff lethal force by either special or conventional forces until the legitimate authority restores order. Consonant with a strategic timetable, SAF and local civilian leaders engineer an education plan targeting progress in key political, social, and

economic areas. SAF also coordinates with local leaders eager to accept private or international investment to build their infrastructure.

SAF intervention should lead to a desired end-state of stability where political, economic, social, and information institutions take root and begin to flourish. SAF will require warriors trained like no others to operate in a complex environment. In the year 2025, warriors will battle for terrain of the mind, performing missions that defy McNamarian precision while protecting American treasure—human life. We propose a blueprint for change to improve existing capabilities. This will require both commitment and time. We do not envision SAF as a quick fix to long-standing problems. Ultimately, making this change requires belief in the possibility of conflict prevention and the dedication to stay the course.

**Notes**

1. *Strategic Assessment 1996, Instruments of US Power.* Institute for National Strategic Studies (Washington, D.C.: National Defense University Press, 1996), 221. The section entitled "New Ways of Applying US Power" stresses "Enhancing the capability of the US Government to exercise influence abroad does not need to mean buying more of the same old product."

2. For the purpose of this paper, we will define *peacespace* as a dimension in which a rough equilibrium exists between a people's expectations and their fulfillment. By dominance, we are not asserting we can control all the variables that occur in peace or during transition to battle. We are saying that given conducive conditions and a catalyst for change, someone can make a difference. Thus, the military constabulary will impose as much control over changing conditions as possible when called upon by national or international leaders to intervene.

# Chapter 1

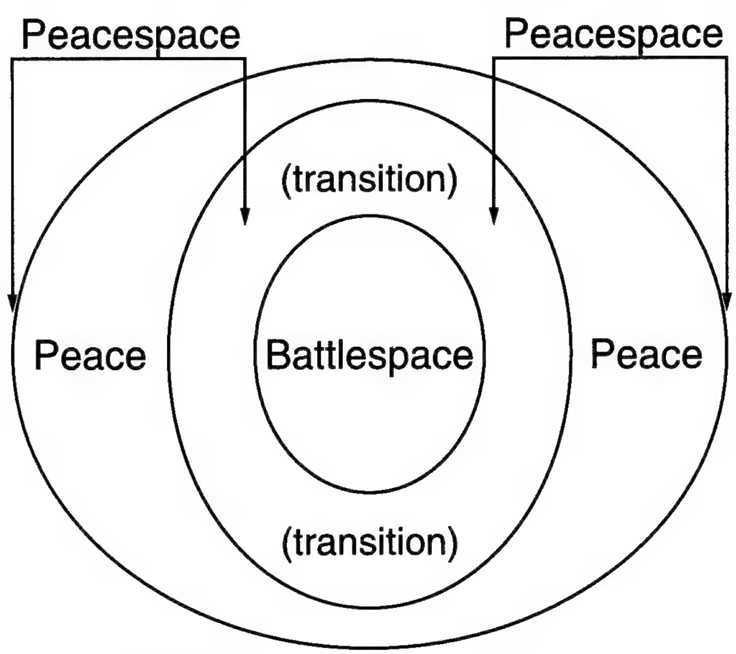
# Introduction

Secretary of Defense William J. Perry outlined his views in a speech entitled "Using Military Force When Deterrence Fails." Specifically, he discussed the new world order emerging as a result of the cold war's cessation and Fukuyama's "end of history."

> Preventing conflict involves creating conditions that make conflict less likely. Like a doctor practicing preventive medicine, we want, if possible, to prevent conditions that provoke conflict from occurring, or at least heal them before they are serious. Some have argued that these efforts are not the business of the Defense Department. I disagree; I call them "defense by other means," and we have launched major programs in the Defense Department to carry them out.[1]

In contrast, Samuel P. Huntington eloquently notes, "the purpose of armed forces is combat."[2] Can US armed forces careen between "traditional" military missions and ill-defined *peacespace* roles without diminishing combat capability?[3]

If peacespace dominance is the "frontier mission of 2025," then it is an orphan no warrior will claim.[4] This mission will be prosecuted in the streets and fields of the developing world, among people ravaged by disease, poverty, hunger, and crime. Battlespace is a condition of warfare requiring at its zenith the application of lethal, combatant military forces—force on force. Warriors organize, train, and equip to fight in the battlespace, not the peacespace—and certainly not in the transition where no true peace exists. Here, only a coercive force holds disgruntled elements in check. The flashpoint (fig. 1-1) denotes a hypothetical




**Source:** Adapted from Field Manual 41-10, *Civil Affairs Operations,* January 1993

**Figure 1-1. Operational Environments**

disturbance somewhere between these conditions we know today as peace and war.

All three circumstances are marked by fluctuating and ambiguous states of conflict, prehostilities, or disputes. In 1996, the military conducts missions in the peacespace without a defined end-state, entry or exit strategies, and doctrine or appropriate technologies. The US military is not organized, trained, or equipped to transition from hunter-killer to nurturer-builder. Rapid or unwieldy transition potentially corrodes US combat capability because it creates confusion in the warrior's mind. Dispelling this confusion is crucial.

Using US national interest as a guide, we can choose if we should act—and if so, where, when, and how. We can consider levels of lethality and appropriateness of response.[5] This paper argues that it is in our national interest to pioneer the peace before it lurches unpredictably into violence. Particular military competencies like order and discipline, organizational skills, and limited liability will likely continue to draw us into the storm.[6]

Pioneering the peace is an appropriate military mission, and it is one we are qualified to undertake. Secretary Perry states, "Some have said that 'war is too important to be left solely to the generals.' Preventive defense says 'Peace is too important to be left solely to the politicians'."[7] In some cases, peacespace dominance need not be a US mission. Other nations or international bodies who have forsworn the use of force might be better suited to these tasks. We advocate organizing, training, and equipping a SAF to provide this capability (table 1). This force would be a composite of both military and civilian personnel, with constabulary (military), education (civilian), and infrastructure (military/civilian) roles (constabulary, education, and infrastructure [CEI]).

Using rules (doctrine) and tools (technology), our challenge is to build a force capable of effecting the desired end-state without sacrificing combat capability. This force will be a catalyst for change. Both the United States and the United Nations have tackled peace missions with mixed results.[9] To secure the success that eluded us in the past requires a different approach. In subsequent chapters, we will analyze the environment, assess the shortfalls in current capability, and propose a solution.

**Table 1**

**Concept Overview**

| | | | |
|---|---|---|---|
| ***Who?*** | SAF (CEI) | SAF/SOF/Conventional | Conventional/SOF/SAF |
| ***What?*** | Conflict Prevention[8] | Conflict Resolution | Conflict Termination |
| ***Where?*** | Peacespace | Transition | Battlespace |

**Notes**

1. The Honorable William J. Perry, secretary of defense, "Using Military Force When Deterrence Fails," *Defense Issues* 10, no. 8 (6 August 1995): n.p. on-line, Internet, 14 May 1996, available from http://www.dtic.mil/defenselink/pubs/di95/di1080.html. Presented during an address to the Aspen Institute Conference.

2. Samuel P. Huntington, "New Contingencies, Old Roles," *Joint Force Quarterly*, no. 8 (Autumn 1993): 39.

3. Part of the dilemma arises from comingling combatant and noncombatant forces in roles that defy traditional definitions. For example, many reservists filling US Army civil affairs billets conduct duties similar to their civilian jobs (i.e., one officer is a high ranking Chase Manhattan Bank official, providing invaluable financial skills during both Haiti and Bosnia operations). Also, medical personnel are typically deemed noncombatants who wear a uniform. This deserves better differentiation in both the law and policy.

4. Despite this assertion, Lieutenant General Zinni, commanding general, I Marine Expeditionary Force, Camp Pendleton, Calif., presented a ***2025*** lecture to Air War College titled "Commanding in 'Frontier Missions'," (Maxwell AFB, Ala.: 29 November 1995). General Zinni supported the Department of Defense (DOD) efforts to preempt conflict by tackling some root causes. However, in 1996, peacespace missions are awkwardly named including peacekeeping, peacemaking, peacetime contingency operations, low-intensity conflict, military operations other than war, *operations*

other than war, or other military operations. The latest RAND© study by Carl H. Builder and Theodore W. Karasik, "Organizing, Training, and Equipping the Air Force for Crises and Lesser Conflicts (CALC)," Project Air Force: 1995, arrives at yet another name for peacespace engagements.

5. USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 33. SAB coins a new word in power projection, *sublethal* which is at variance with DOD which employs the term *nonlethal.* Whatever the outcome of the semantic discussion, this paper will employ both definitions (i.e., nonlethal and sublethal versus lethal) to describe incremental increases in power. Effectively, nonlethals should be exactly that—not lethal. Sublethal is that force or power just below lethal deadly force.

6. The Feres Doctrine espoused by the Supreme Court in 1950 limits the liability of the US government in the event of a service-related death. (340 USC 135—1950) This limitation applies to military personnel only. With the shift of certain critical tasks to civilians, either civil service or contract, the liability issue must be addressed for civilians in hazardous zones.

7. Perry, remarks delivered to the John F. Kennedy School of Government, Harvard University, on-line, Internet, 13 May 1996, available from http://www.dtic.mil/ defenselink.

8. Dr Larry Cable, "The End-State: Why Nations Stop Fighting," lecture, Air Command and Staff College, Maxwell AFB, Ala., 16 January 1996. Dr Cable is an associate professor of history at the University of North Carolina, Wilmington. Additionally, he is a frequent guest lecturer at the USAF Special Operations School (USAFSOS), Hurlburt Field, Florida. Additionally, Dr Cable was in the US Marine Corps during the Vietnam War. He is the 1995 Gen James H. Doolittle Award recipient at the USAFSOS, awarded to the School Educator of the Year. In numerous meetings, Dr Cable differentiated between current policy, doctrine, and missions, which essentially deal with conflict termination, and conflict prevention or resolution.

9. Steven L. Canby, "Roles, Missions, and JTFs: Unintended Consequences," *Joint Force Quarterly,* no. 6 (Autumn/Winter 1994–1995): 68–75.

# Chapter 2

# World Trend

*They make a wilderness and call it peace.*

—Tacitus

The US military is heavily taxed, in 1996, performing peace operations throughout the world. Such commitments will likely increase. Thinkers like Robert Kaplan, Thomas Homer-Dixon, and Martin van Creveld strongly believe the world will suffer a number of pandemic problems in 2025: overpopulation, ecological disasters, severe water shortages, rampant disease, and refugees on the march.[1] Strands of these alarmist visions exist today in Africa, South Asia, and China. Robert Kaplan argues the United States may ignore these regional crises at its own risk. Will governments, unable to cope with epidemic problems, simply disappear?[2]

Compounding the specter of "national dissolution" is a population growth from 5 billion in 1996 to nearly 8 billion in 2025—over 7 billion will reside in less-developed regions that in 1996 cannot produce enough food to feed their people.[3] Worse, previously eradicated communicable diseases, such as tuberculosis and influenza, are mutating and spreading.[4] These new and developing strains are airborne and resistant to antibiotics.[5]

Desertification and deforestation are causing populations to flee to cities, making criminal anarchy the real strategic danger. Kaplan describes the worst of its victims: "Young men [are] like loose molecules in a very unstable social fluid, a fluid . . . clearly on the verge of igniting."[6] This increasing propensity to violence is partially mirrored by US crime statistics. Between 1985 and 1992, the murder rate for 14–17 year-old males doubled for whites and increased by more than 300 percent for African-Americans.[7] In the year 2000, the number of youths aged 14–17 will increase by 500,000 in the US alone—effectively, each subsequent generation is three times more dangerous than the one preceding it.[8]

Homer-Dixon believes the environment is "*the* national security issue of the early 21st century" (emphasis in original).[9] He predicts future wars and civil violence may arise from the scarcity of such resources as water, cropland, forests, and fish.[10] Huntington warns of wholesale tribal conflict.[11] He pictures a world in which democratic liberalism gives way to a darker Hobbesian world—Hegel and Fukuyama's "last man" supplanted.[12] While these polemicists paint a bleak landscape, perhaps the change will be more gradual and evolutionary. Just as these forces are irretrievably affecting the world, movements are underway to change the way we fight wars.

## Battlespace Trend

*To many men . . . The miasma of peace seems more suffocating than the bracing air of war.*[13]

Since World War II (WWII), warfare has both changed and remained chillingly the same. The collapse of colonial empires resulted in nearly 200 nation-states, many of them small, unstable, and vulnerable. According to van Creveld, "Judging by the experience of the last two decades, the visions of long-range, computerized, high-tech warfare so dear to the military-industrial complex will never come to pass. Armed conflicts will be waged by men on earth, not robots in space."[14] He also implies that warfare will be frequent in the

developing world: "In light of the fact that 95 percent of the earth's population will be in the poorest areas of the globe, the question is not whether there will be war (there will be a lot of it) but what kind of war. And who will fight whom?"[15]

Van Creveld speaks of conflicts which require conventional, special operations, and peacespace warriors. Whenever the US engages in these situations, certain trends in the US domestic arena will both constrain and empower future force structure. We must understand these trends to accurately determine force composition for 2025.[16]

## Domestic Trend

*War is hell, but peace is a pain in the ass.*[17]

An emerging domestic trend is America's aversion to casualties.[18] Any future military planning must take this into account. The death of 18 soldiers in Somalia effectively ended that mission. One death in Bosnia received national attention. Preoccupation with prisoners of war in Vietnam, friendly-fire incidents, and the expectation that precision strikes will limit collateral damage—all these result in the conclusion that there is simply less room for error, particularly in missions of questionable vital national interest.

The competing demand for fiscal resources is also likely to increase. At some point, the US appears to have no options other than to either narrow its interests or act before a situation requires large injections of armed force. These choices are especially important in light of the high operations tempo characterized by the first three years of the Clinton administration.[19] Force readiness and retention will be contingent on addressing the future conflict set.[20] Three recent expeditions into peacespace illuminate both lessons learned and current shortfalls facing leaders and planners.

### Somalia

Graphic evidence of famine, provided by the Cable News Network (CNN), triggered the intervention in Somalia.[21] At no time did anyone portray the Somalia relief mission as in the national interest. According to one analyst, the military and civilian agencies had little entry criteria—only that the US had the means to act and so should.[22] Subsequent events expanded the US involvement to a force of 28,000. Their task was to suppress the violence and relieve interruptions in the delivery of aid. Gradually, the United States, operating in conjunction with the UN, became involved in a nation-building effort for which some believed the military was ill-suited. This mission was abruptly aborted with the deaths of 18 soldiers in October 1993.[23] Among the many lessons drawn from the Somalia engagement: we conclude that the lack of clear entry and exit criteria combined with foggy rules of engagement to inhibit a successful mission.[24]

### Haiti

An influx of refugees, not famine, triggered the 1994 US intervention in Haiti. Haitian citizens, attempting to escape violence, political instability, and economic chaos, flooded our shores.[25] Thus, some criteria for intervention were used and the operation appears to have been in the national interest. US involvement in Haiti included an effort to legitimize President Jean-Bertrand Aristide's government and restore democracy through the use of military forces. One CINC cited Haiti as evidence for the notion of training warriors for missions of violence and—literally within the space of an airplane ride—changing them into police and peacekeepers.[26] During Operation Provide Hope, military forces used radio and television broadcasts, leaflet drops, and personal contacts to educate Haitian citizens on democracy. US Army Civil Affairs units trained Haitian government officials, established judicial courts, and developed a governmental

system.[27] US forces performed infrastructure development duties by "reinitiating legitimate civil functions . . . public activities, water, electricity, sanitation, medical, [services], food, public information, town meetings, broadcasts, and monitoring the local Haitian army and police."[28] These actions created environments where economic growth could occur. Even so, these activities do not mean that careful planning is institutionalized or that successful execution is certain.

### Bosnia

The Bosnia mission was one of the more carefully considered US interventions to date; it effectively blended ground, naval, and air forces in support of peace.[29] Careful debate centered on US national interests in the former Yugoslavia. Attention concentrated on the utility of inserting ground forces between warring factions. Ultimately, airpower brought contending groups to the bargaining table.[30]

> The precision of the NATO coalition's attacks last summer altered the course of that three-year war, resulting in the Dayton peace talks and preventing the conflict from spilling over into other countries. This force was effective, ultimately, because it was applied towards clear, achievable policy objectives, in effective coordination with other diplomatic tools, with a clear view of military requirements.[31]

Airpower also limited violence by creating no-fly zones. Naval craft enforced the arms embargo in the Adriatic in Operation Sharp Guard.[32] After brokering a peace settlement, army units provided essential ground forces to secure the peace.

## Summary

This chapter reviews world trends that increase the range of actions in support of peace. Battlespace will include both major regional contingencies and excursions into low-level conflict. Peacespace dominance may mean working problems before they boil over into war. "If we can prevent the conditions for conflict, we reduce the risk of having to send our forces into harm's way to deter or defeat aggression."[33] As our recent experiences in Somalia, Haiti, and Bosnia demonstrate, we have difficulty operating in and transitioning back into peacespace. These operations provide important lessons for devising rational entry and exit criteria.

> It is also true that if we move early in dealing with these conflicts, and if we have an effective method for carrying out international peace enforcement, especially in a preventative way, we have a new tool which can help in the early resolution of enormously difficult, potentially intractable situations that could well offset our national interests and our future.[34]

In the next chapter, we will propose the most efficient way to defend our national interest: act before a situation flares into violence. We will propose a force to act as a catalyst for change to dampen violence and orchestrate peace.

**Notes**

1. Robert D. Kaplan, "The Coming Anarchy," *The Atlantic Monthly*, February 1994, 44–76; Thomas Homer-Dixon, "Environmental Change and Violent Conflict," *Scientific American* 268, no. 2 (February 1993): 38–45; Martin van Creveld, *The Transformation of War* (New York: Free Press, 1991), 192–223.

2. Kaplan, 44–76.

3. Lawrence C. Hellman, PhD, "Humanitarian Operations," lecture, Air Command and Staff College, Maxwell AFB, Ala., 19 January 1996. Dr Hellman is a consultant to USAID, and data included was used by permission. Additionally, Dr Armin Ludwig, "Ecosystemic Violence," ***2025*** program lecture, Air War College, Maxwell AFB, Ala., 6 September 1995. Dr Ludwig presented a fascinating picture of population, net primary production, and the world's ability to feed itself given current trends in population growth. His computations did not include the potential effects of genetic engineering (plants that grow in arid or saline soils), synthetic soils, or biogenetic plant species development (higher yield, greater yield per year, yield of cross-fertilized varieties, etc.). On the balance, he caveated each condition or phenomena with a caution to address the consequences of actions which "tamper" with nature (e.g., fertilizers and irrigation practices).

4. Anita Manning, "Viruses Mutate among Underfed," *USA Today*, 17 April 1996, 1. Malnourished people and animals may provide a breeding ground for mutant viruses that can then infect others. Dr Orville A. Levander, a nutritionist with the US Department of Agriculture, concludes, "We are not protected from

what might be happening to malnourished people in Africa." The World Health Organization report, "The Tuberculosis Epidemic 1996: Groups At Risk," states:

> In 1995, more people died of TB than in any other year in human history. It kills more adults than all other infectious diseases combined. Multidrug resistance is growing, threatening to make TB incurable again. Since issuing the global warning three years ago, some initial steps have been taken but they are dangerouslly insufficient. Tuberculosis cannot be controlled in some parts of the world and left to spread in others. Tuberculosis is a global epidemic that requires a unified, global response.

5. Kaplan, 44–76.

6. Ibid., 46.

7. In "Moral Poverty," John Dilulio writes, "Americans are sitting atop a demographic crime bomb." *The Chicago Tribune*, 15 December 1995, section 1: 31. If the US is to effectively engage abroad, many of these systemic social problems must first be correctly addressed. The thesis of this paper assumes the US will successfully correct many internal problems in the next 30 years.

8. Ibid. Peter Schwartz discusses the opportunity and dilemma presented by the "Global Teenager" in *The Art of the Long View* (New York: Currency Doubleday, 1991), 124–40. Comparing the current demographic trends with projected population trends, he notes "Barring widespread plague or other catastrophe, there will be over 2 billion teenagers in the world in the year 2001. That's *fifty* times the number of teenagers in America in the peak years of the baby boom." The "Global Teenager" existence will be a driving force. However, Schwartz does not see this driver in a wholly negative vein, particularly with respect to education.

9. Homer-Dixon, 38–45.

10. Ludwig and Homer-Dixon assert growing scarcities of renewable resources can contribute to social instability and civil strife.

11. Samuel P. Huntington, "The Clash of Civilizations?" *Foreign Affairs* 72, no. 3 (Summer 1993): 22–49.

12. Francis Fukuyama, *The End of History and the Last Man* (New York: Free Press, 1992), 287–328.

13. George Steiner. French-born US critic and novelist. "Has Truth a Future?" Bronowski Memorial Lecture, 1978. *The Columbia Dictionary of Quotations* (New York: Columbia University Press, 1993). Microsoft® Bookshelf.

14. Van Creveld, 212.

15. Kaplan, 73.

16. Colin S. Gray, "The Changing Nature of Warfare?" *Naval War College Review* 69, no. 2 (Spring 1996): 13–14. Gray cites information from Edward N. Luttwak, *Strategy: The Logic of War and Peace*, as follows: "War, in common with sport, has the characteristic that what worked yesterday may not work tomorrow, precisely because it worked yesterday. Nothing tends to fail like success."

17. Quoted in "A SIOP for *Perestroika*?" by Col Richard Szafranski in a research report (Maxwell AFB, Ala.: Air University, Air War College, 1990), 1. James Schlesinger made the statement on a *Face the Nation* edition.

18. Eric V. Larson, "Casualties and Consensus: The Historical Role of Casualties in Domestic Support for US Military Operations" (Santa Monica, Calif.: RAND©, 1996), iii, 102–3. Larson provides a comprehensive look at the role of casualties in administering public policy.

> The relationship between US casualties and public opinion on military operations remains an important yet greatly misunderstood issue. It is now an article of faith in political and media circles that the American public will no longer accept casualties in US military operations and that casualties inexorably lead to irresistible calls for the immediate withdrawal of US forces. If true, this would not only call into question the credibility of the US Armed Forces in deterring potential adversaries but would be profoundly important in decisions regarding the country's strategy, alliance, and other commitments, force structure, doctrine, and military campaign planning.

However, Larson concludes the public support or lack thereof is more accurately a reflection of the US leadership position and disagreements among key political figures. "As the historical record shows, attributing declining support solely to casualties misses the real story." When the public perceives benefit, they will exhibit a high tolerance for casualties. Also, Colin Gray argues as follows in "The Changing Nature of Warfare?" *Naval War College Review* 69, no. 2 (Spring 1996): 10–11.

> It is true that a machine-rich American culture has looked sensibly to maximize the roles of vehicles, steel, and explosives in lieu of human flesh whenever appropriate—and sometimes beyond that point. But it is also true, contrary to popular mythology, that when the stakes are very high, as in the Civil War and the two world wars, the United States has no tradition of being especially sparing of American lives.

19. Operations and personnel tempo for some USAF weapons systems and respective personnel reached crisis proportions by 1994. General Fogelman, CSAF, instituted a process to track and reduce this to below 120 days. On 17 April 1996, AF/XOOOR (Major Fink) passed the following figures to the authors for frame of reference.

| USAF Weapon System PERSTEMPO (average # days TDY/crew/year) | 1994 | 1995 | 1st Qtr 1996 |
|---|---|---|---|
| HC-130 (rescue) | 194 days | 135 days | 38* days |
| EC-130E (ABCCC) | 186 days | 175 days | 29* days |
| E-3 (AWACS) | 162 days | 129 days | 24 days |
| U-2 | 148 days | 148 days | 36* days |
| RC-135 (Rivet Joint) | 143 days | 161 days | 37* days |
| EC-130H (Compass Call) | 104 days | 123 days | 54* days |
| HH-60G USAF rescue Pave Hawks | 53 days | 116 days | 28* days |
| Special Operations Forces (SOF) | | | |
| AC-130 Spectre Gunship | 159 days | 83 days | 25 days |
| MH-53J Pave Low | 134 days | 74 days | 23 days |
| MH-60G SOF Pave Hawk | 158 days | 106 days | 30* days |
| Combat Control Teams (CCT) | 186 days | 160 days | 39 days |

*Continuing at 28 days and higher will exceed the 120-day limit for the year.

The Navy, Army, Marine Corps, and US Special Operations Command provided similar data which is submitted to the Joint Staff as part of the Joint Monthly Readiness Review. Of particular interest currently are all units designated as "low density/high demand" or LD/HD. In addition to some of the Air Force systems and units above, Army civil affairs and psychological operations battalions, Patriot missile batteries, Navy Seabees, and SEALs receive additional scrutiny in this category. While specific data is classified, the following general trends are provided for comparison. USMC 1 MEF wings average 160 days deployed per year for training deployments; divisions average 145 days deployed. Some USN surface combatants, amphibious ships, fast attack submarines, and aircraft squadrons range for 10–40 percent above the maximum chief of naval operations PERSTEMPO program goals. These goals are (1) a maximum deployment of six months, portal to portal, (2) a minimum turn-around ratio of 2:1 between deployments (if out six months, should be in port 12 months before going afloat again), and (3) a minimum of 50 percent time in home port for a unit over a five-year period (three past years and two projected years). Roughly, the Navy numbers equate to 180 days over 18 months or 120 days per year. USSOCOM provided detailed data for special operations personnel, many of whom are deployed well above the 120-day goal. In US Army Special Operations Command, special forces and civil affairs officers average 180 days deployed per year. In Naval Special Operations Command, SEAL team corpsmen and officers average 175 and 163 days respectively. AC-130H navigators average 184 days and pararescuemen (PJ) average 168 days from Air Force Special Operations Command.

20. "World View: The 1996 Strategic Assessment from the Strategic Studies Institute," ed. Earl H. Tilford, Jr. (Carlisle Barracks, Pa.: US Army War College, 1996), 3–4.

21. Cable News Network (CNN)® is an affiliate of Ted Turner Productions, Atlanta, Ga.

22. Kenneth Allard, *Somalia Operations: Lessons Learned* (Washington, D.C.: NDU Press, 1995), 89.

23. Ibid., 30. Also see Col F. M. Lorenz, USMC, "Forging Rules of Engagement: Lessons Learned in Operation United Shield," on-line, Internet, 10 March 1996, available from http://www.cgsc.army.mil/cgsc/milrev/95novdec/lor.htm.

24. Lorenz, Internet, http://www-cgsc.army.mil/cgsc/milrev/95novdec/lor.htm.

25. W. Darrent Pitts, "A Guantanamo Diary—Operation Sea Signal," *Joint Forces Quarterly*, no. 9 (Autumn 1995): 118. Operation Sea Signal was a humanitarian mission designed to care for over 14,000 Haitian refugees at the US Guantanamo Naval Base, Cuba. Overwhelmed civil affairs personnel were unable to deal with subhuman camp conditions. Linguists were in short supply.

26. Address to Air War College. Academic privilege applies to this source.

27. "United States Special Operations Forces Posture Statement," 1994, 26–27.

28. Sqn Ldr Sam Allotey et al., "Planning and Execution of Conflict Termination," a Research Paper presented to the Directorate of Research, Air Command and Staff College (Maxwell AFB, Ala.: Air University, Air Command and Staff College, May 1995), 83.

29. As it took four years for the US to engage in Bosnia, presumably we preceded our actions by

pragmatic and thoughtful preparations to correct the perceived deficiencies of the UN operations.

30. George C. Wilson, "A Lesson in Peacekeeping," *Air Force Times*, 11 March 1996, 54. Wilson, a former defense correspondent of *The Washington Post* and author of several military affairs books, discusses a "presence" maneuver used by Adm Leighton Smith, NATO commander in Bosnia-Herzegovina. F-18 Hornets scrambled from the USS *George Washington* in response to the shelling of Malaysian military in "B-Hatch." When the Malaysians did not "come up" on frequency to direct the bomb drop or missile launch, the Navy pilots converted to a "presence" maneuver—a major part of NATO's strategy for peacekeeping in Bosnia-Herzegovina. Dropping to 10,000 feet, the pilots advanced throttles to make more noise with their engines. The resultant thunder stopped the shelling of Malaysians. Lt Bill Lind, USN, quipped, "It's called peace through superior volume." The deterrence works because the planes *have* dropped bombs. These tactics are essentially ad hoc in nature and not planned in advance.

31. The Honorable Sheila Widnall, secretary of the Air Force, "AF Evolving Through Contacts With Other Nations," MSgt Gary Pomeroy, Air Force News Service, on-line, Internet, 15 May 1996, available from http://www.dtic.mil/defenselink.

32. Information of Operation Sharp Guard found on-line, Internet, 15 May 1996, available from http://www.nato.int/ifor/general/shrp-grd.htm.

33. Perry, remarks delivered to the John F. Kennedy School of Government, Harvard University, on-line, Internet, 13 May 1996, available from http://www.dtic.mil/ defenselink.

34. Joint Warfighting Center, "Joint Task Force Commander's Handbook for Peace Operations," *Air Command and Staff College War Termination Coursebook* (Maxwell AFB, Ala.: Air University Press, 1996), 64.

# Chapter 3

# Concept Description

*We conducted such operations [operations other than war] during the Cold War, but they were few and far between. And frankly, we did not always do them very well. So we lack a time-tested template that we can lay down every time we commit to one of these operations.*

—Gen John M. Shalikashvili

The template requested by the chairman of the Joint Chiefs is a complex one. The propensity for oversimplification often leads us to reduce the template to a "boilerplate." Leaders and planners require more. This chapter covers a proposal for a small, rugged, and specialized composite force dedicated to creating and operating in the physical and psychological state we call the peacespace. The proposal moves from situation assessment and enabling doctrine (rules) and technology (tools) to SAF core capabilities.

## Situation Assessment

Some triggering mechanism currently launches excursions into peacespace. This may be public opinion, a UN resolution, or perceived national interest. In 2025, national or international authorities will still judge whether or not to intervene. This assessment should use clear criteria meant to assess the prospects for success in creating a better state of peace.[1] Candidates for intervention might be identified by spikes or flash points which erupt on a digital cultural map as "boundary" lines are penetrated.[2] Figure 3-1 illustrates our vision of the digital cultural map.

**Figure 3-1. Digital Cultural Map**

Using technology, a digital cultural map (DCM) could decrease peacespace ambiguity and aid leaders responding to conflicts or crises by sorting disparate data. It would "navigate" the geopolitical globe in a manner similar to an aircraft navigation digital map, blending together a multitude of diverse databases in visual or graphical interface. These candidates for intervention can be prioritized or "triaged" using basic, yet flexible criteria. Appendix A gives detailed intervention criteria.

The National Security Council (NSC) or the United Nations would evaluate the situation and classify the case as (1) costly, (2) borderline, or (3) clear-cut candidate for intervention. For example, the DCM assigns values which indicate candidate "A" has a high level of violence, an inadequate political or social climate, and a deteriorated infrastructure. This case may very well be categorized as too costly, regardless of perceived importance to national interest. Candidate "B," on the other hand, has a moderate level of violence that could be

quelled by nonlethal technologies and a well-trained constabulary force. Its social and political institutions are minimally deteriorated, lending credence to education efforts. Finally, its infrastructure is capable of rejuvenation, leading to optimism that private investment might prove successful.[3] Figure 3-2 depicts intervention candidates and correlates them to specific criteria.

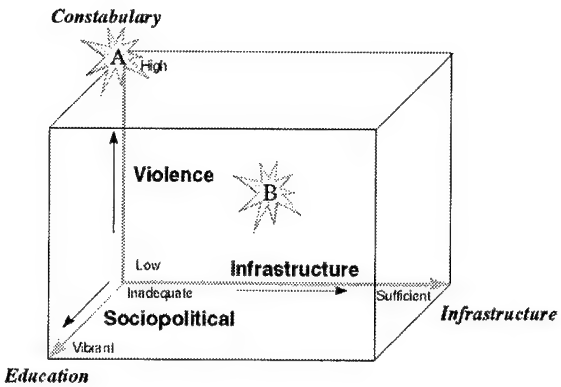



**Figure 3-2. Intervention Candidates**

Ultimately, leaders make the decision to intervene, using subjective judgments: (1) Is the intervention in US or UN interests? (2) Is the desired outcome worth the cost? (3) Is SAF the appropriate force? (i.e., Does open violence currently exist? Can SAF establish a secure environment or are more conventional forces appropriate?) (4) What timetable exists for achieving objectives? (5) Do we have measures of merit for success or withdrawal?[4] The decision is made either to intervene or not. The same objective and subjective criteria can determine when goals are met and an exit is appropriate. They can also demonstrate when an operation is stalled and should be abandoned. This paper asserts that the current force structure does not adequately meet the tasks at hand. The SAF concept, beginning with doctrine and tools, is one alternative to accomplish this mission.

**Rules and Tools**

The first step required in building this new force is to make "rules." Doctrine covers many aspects of policy from the national security strategy level to tactical employment. While a comprehensive doctrine is beyond the scope of this paper, initial thoughts regarding doctrinal changes for implementing SAF are appropriate.[5]

**Flexibility/versatility**. The dynamics of intervention missions demand a fresh approach to each operation. To avoid overlaying "previous experience" inappropriately, every operation must be tailor-made and sized to the situation. Just as civilian industry is innovatively exploiting niche markets, "tailoring" manufacturing on a mass scale, SAF must flex great power on a small scale.[6]

**Concentration**. CEI efforts need teeth in order to ensure credibility. These functions seek to affect whole societies and will require a complete fidelity of purpose. The small, rugged, mobile, and composite structure of SAF encapsulates the notion of concentration of effort. SAF launches an offensive by attacking the causes of conflict before they erupt into hostilities. Conflict prevention also provides economy of force by limiting the application of violence and reducing the chance of escalation.

**Persistence**. CEI efforts should be comprehensive, coordinated, far-reaching, systematic, and applied until they succeed or the decision is made to withdraw. The appeal of airpower to SAF is the ability to persist in end-state efforts until established goals are achieved.[7] While airpower may reduce risks and increase effectiveness of both land and sea components, success in peacespace operations lies in balanced air, land, and sea dominance.

By design, we have only hinted at the doctrinal possibilities.[8] Even if further exploration and developments lead to a "virtual" presence in the peacespace, someone will still require technology or tools to achieve their goals and objectives in 2025. Parallel to formulating doctrine is

determining what tools SAF needs to perform its mission. Embedded in the CEI concept are potential technologies to enable SAF forces.[9]

## Constabulary, Education, and Infrastructure (CEI) Concept

The integrated use of CEI provides a foundation for dampening conflict and promoting stability. Certain characteristics are crucial to success: appropriate doctrine (carefully matched technologies), small force structure (4,000–10,000 total active and reserve component mix), mobility, ruggedness, and specialization.[10] The elements of CEI are discussed in the following pages.

### Constabulary

One of the commander's first concerns in entering a SAF engagement will be to impose order while protecting the participants. Builder defines *constabulary* as an "armed police force organized on military lines but distinct from the regular army."[11] The constabulary envisioned is primarily composed of military forces who dominate situations of lawlessness. If levels of violence escalate, SAF constabulary forces could temporarily pass control of the situation to stand off "guardian" systems.[12] As another option, SAF could direct increasing levels of lethal force until order is restored. In extremis conditions require clean handoffs between SAF and either special operations or conventional combat forces.

As in battlespace dominance, peacespace constabulary actions can occur in serial or parallel with education and infrastructure, similar to battlespace dominance.[13] Effects and effectiveness will depend on a variety of nonlethal, sublethal, and lethal technologies integrated with effective command and control to create an environment conducive to long-term development.[14]

### Lift

Airpower and space power capabilities could significantly enhance the constabulary force. Reacting to violent situations will require delivery of either forces or equipment—anytime, anyplace. Some lift requirements mirror those of today; for example, moving SAF or civilian forces and their equipment, or delivering food, water, fuel, and medicine. Although we anticipate significant improvements in capability, survivability, and reliability, these subjects are adequately covered in other studies. Table 2 depicts SAF's unique mission, objectives, and potential technologies.[15]

Potential technological advances should address current shortfalls in airlift capability. Perhaps the innovative low altitude parachute extraction system (LAPES) tactic of the twentieth century will spawn equally creative solutions in 2025, such as the precision/large-scale airdrop technologies listed in table 2. The Special Operations Forces Vehicle,

**Table 2**

**Lift Objectives and Technologies**

| MISSION | OBJECTIVE | TECHNOLOGY |
|---|---|---|
| Lift | Mobility<br>• Transship SAF forces and equipment<br>• Transship NGO/PVO people/equipment<br>• Supply infrastructure/education"stuff"<br>• Deliver food/fuel/medicine | • Tiltwing super short takeoff and landing Advanced theater transport (TSSTL/ATT)<br>• Heavy lift aircraft with mission Pod<br>• Low observable transport<br>• Precision/Large scale airdrop<br>• Global Navigation System |
| SAR | Vertical lift extraction of SAF ground troop | • SOF vehicle<br>• Advanced personnel locators |
| Resupply | Replenishment | • Precision/Large scale airdrop<br>• Advanced material handling equipment |

listed as a search and rescue (SAR) technology, is a potential CV-22 follow-on aircraft (1500nm range, high subsonic speed, low-observable technologies). This vehicle may allow vertical extraction of SAF ground forces when required. Additionally, rapid identification of threats to ground operations could allow calmative agent application from a low-altitude (atmospheric), orbital unmanned aerial vehicle (UAV).[16] Thus, accurate identification of threats is a key enabler. Figure 3-3 displays the employment of some required lift technologies.

advances in intelligence, surveillance, and reconnaissance.

**Advanced Intelligence, Surveillance, and Reconnaissance**

One centerpiece of SAF is that of amplifying the efficiency of what should be a small force. We can accomplish this by providing highly detailed and timely intelligence or information.[18] The needs of SAF are not particularly unique—they mirror those of combat forces. Current intelligence, surveillance, and reconnaissance (ISR) needs will persist; the challenge will be to pursue technologies and develop processes that create advanced ISR appropriate to SAF requirements in 2025.

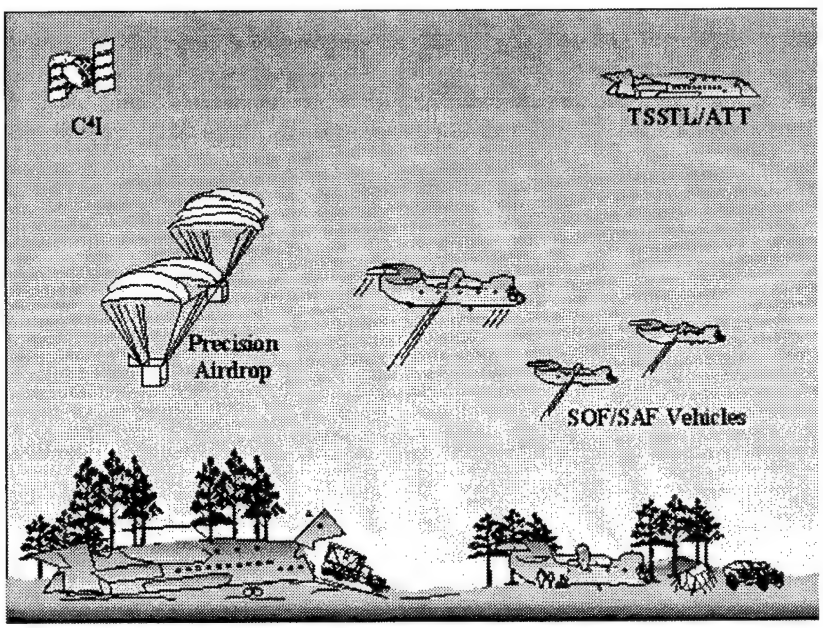



**Figure 3-3. Lift into Peacespace**

While required items could be either strategically prepositioned or vertically hoisted in by CV-22 or follow-on aircraft, we could also deliver them to littoral regions by sealift for overland transport.[17] Regardless, these and other infrequent loads will require rapid delivery under unusual or extreme circumstances. SAF forces and planners could identify alternative solutions to either infrastructure requirements or planned lift acquisitions through early identification of known military shortfalls and limitations. Getting people and material to the right place at the right time will also necessitate

Three principles govern ISR in the peacespace: timeliness, accuracy, and precision. Peacespace dominance will drive an increased reliance on information residing primarily in open sources. Timeliness drives a need for on-scene information acquisition (fig. 3-4). Sensor-laden UAVs or ultralight aircraft platforms could be the workhorse of SAF's advanced ISR toolkit. Advanced ISR, contributing to "information dominance,"

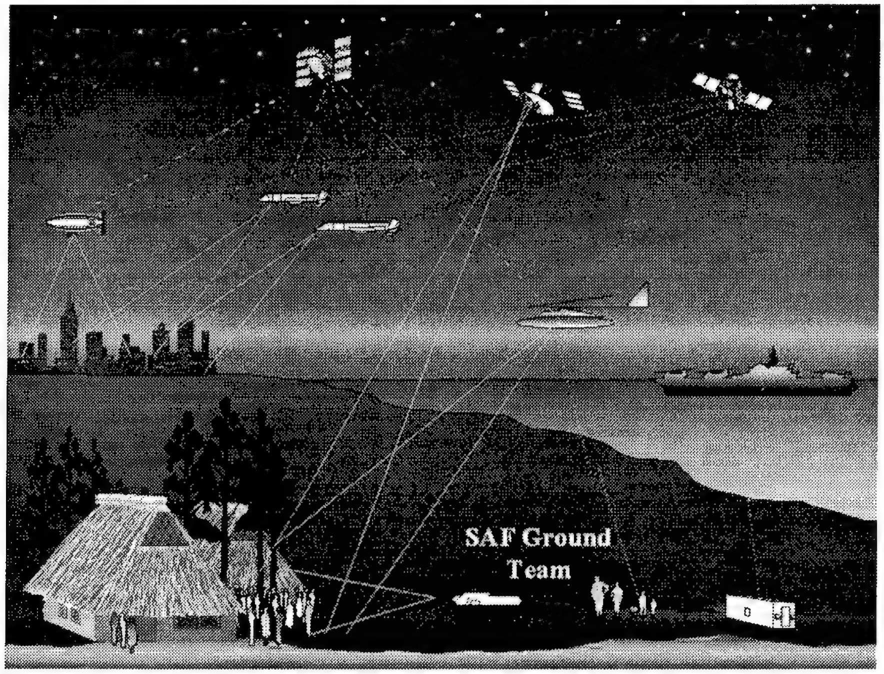



**Figure 3-4. Advanced ISR in the Peacespace**

will allow a limited number of ground troops to leverage their coercive capability.

Accurate intelligence could allow leaders to identify and preempt trouble before it becomes conflict. Analysis could come from nontraditional agencies, including the departments of Commerce, Treasury, State, and Agriculture; the Center for Disease Control; the World Bank or the International Monetary Fund; Save the Children; Doctors Without Borders; and Greenpeace. Coupled with open-source intelligence, wider use of human intelligence will help us know intentions as well as capabilities—the precision index.

> Rather than detecting and analyzing jet aircraft which emits [sic] a familiar visual, infrared, and telemetry signal . . . the intelligence community may have to detect and analyze old, small aircraft transporting drugs. Rather than spotting tank battalions in movement, it may have to spot guerrillas. And rather than dissecting a Soviet arms-control proposal, it may have to assess a country's attitude toward terrorism.[19]

Centralized intelligence can provide details on weapons movements and violent elements. Count de Marenches, former chief of French intelligence, stated, "Precision personal intelligence can be more critical than precision-guided munitions."[20] The vast amount of information will have to be culled in order to monitor the movement of aggressors. Their religious and cultural views must also be monitored. Information must be accurate, digestible, and relevant.

> The best satellites can't peer into a terrorist's mind. Nor can they necessarily reveal the intentions of a Saddam Hussein. Satellites and other technical surveillance technologies told the United States that Saddam was massing troops near the Kuwait border. But the United States—short on spies in Baghdad's inner circles—brushed aside such warnings as alarmist and mistakenly concluded the troop movements were just a bluff. One human spy in or near Saddam's inner circle might have cast light on his intentions and changed history.[21]

As a result of this enormous need for contextual intelligence, the attendant command, control, communications, and computers ($C^4$) support will be immense. Table 3 depicts advanced ISR/$C^4$ objectives and technologies.[22]

**Table 3**

**Advanced ISR/C4 Objectives and Technologies**

| MISSION | OBJECTIVE | TECHNOLOGY |
|---|---|---|
| Advanced ISR | • Strategic: feeders to NCA DCM<br>• Operational: SAF requirements<br>• Tactical: output/effects based targeting<br>• Surveillance/Target ID: UAV constellation | • Long endurance UAVs/UTAs<br>• Unmanned mini helos<br>• Target reporter<br>• Unattended ground sensors<br>• Weather surveillance and prediction<br>• Low-cost space-based surveillance<br>• Virgual presence |
| $C^4$ | Reliable, high fidelity, robust | Scavenge $C^4$ solutions from expert sources |

## Command, Control, Communications, and Computers

The peacespace mission is also based on conflict prevention or resolution, which dictates accurate communication with local leaders. Improvements in computer voice recognition technology may permit the development and fielding of translators for installation on board the UAV or ultralight. By 2025, real-time broadcast of instructions via remote transmission might obviate the need to develop large forces of language experts. We can leverage a small cadre of linguists remotely. This capability also would increase the effectiveness of both the psychological operations team and the education/infrastructure mission.

Finally, SAF will require data links to rear areas to provide recurring information and updates. This requirement is an entry point of SAF to the "metasystem."[23] SAF must tie into other $C^4$ systems for point-to-point communications. The concept might be along the lines of an Iridium® system potentially placing more than 50 dedicated satellites in a low-earth orbit (LEO).[24] Essentially, SAF requires reliable communications to any individual with the correct equipment and cryptologic material or device, particularly while performing the envisioned air dominance role.[25]

## Air Dominance

To provide a viable constabulary force for 2025, Builder notes certain technological challenges.[26] First, the constabulary must immediately identify, engage, and suppress certain kinetic weapons. Current methods of counterbattery fire, which result in area barrages of suspected gun emplacements, do not provide the surgical strike capability required to ensure engagements with limited collateral effects.

Additionally, the problem of mobile kinetic targets burdens the conventional lethal forces. SAF must solve this equation effectively in the most difficult terrain—urban environments—to limit collateral damage and assure a "fire-free" zone. Figure 3-5 graphically depicts one solution to this problem. Additionally, we have outlined air dominance missions, objectives, and technologies in table 4 below.[27]

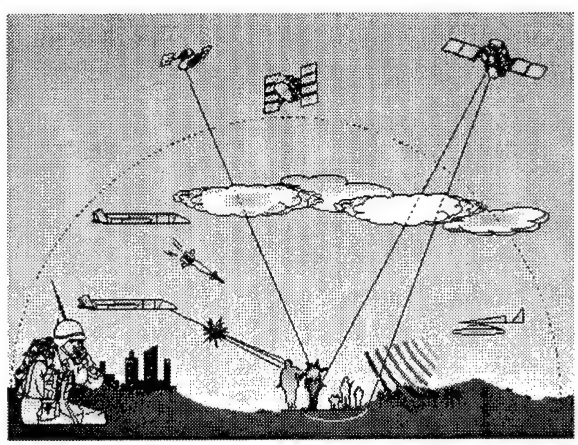


**Figure 3-5. Security Assurance Force Fire-Free Zone**

**Table 4**

**Air Dominance Objectives and Technologies**

| MISSION | OBJECTIVE | TECHNOLOGY |
|---|---|---|
| Air dominance | Deterrence, law and order | • UAV/ultralight configured with LifeGuard<br>• Antisniper probability device<br>• Suppress hostile artillery<br>• Laser Antisensor Weapon |
| Air dominance | Urban assault | • Helo vehicle hybrid |
| Air dominance | Psychological operations | • UAV configured as replacement EC-130 |
| Air dominance | Weapons delivery (lethal & nonlethal) | • UAV with rocket launchers, EMP, microwave, lasers<br>• Pyrotechnic Electromagnetic Pulse<br>• RF warhead |
| Air dominance | Survivability | • UAV configured with chameleon concept<br>• Full body armor |
| Air dominance | Command and control | • Holographic $C^2$ Sandbox (also applicable to $C^4$ section) |

The air dominance mission will be significantly enhanced by certain technologies. For example, Lawrence Livermore Laboratories developed a system—LifeGuard—which provides accurate computerized thermal bullet tracking.[28] Less than 300 milliseconds (ms) after an incoming round is fired, LifeGuard gives a track back to the point of fire. Pinpointing the "shooter" allows direct application of lethal, sublethal, or nonlethal means to apprehend the individual or entity and deter others. SAF forces would mount the LifeGuard system on one of several UAVs and ultralights operating in a constellation over the target area. Constellation configuration is tailored to the environment, taking into account urban or desert terrain (fig. 3-6).[29]

While rapid reconfiguration of the UAVs for tailored employment is a linchpin to this

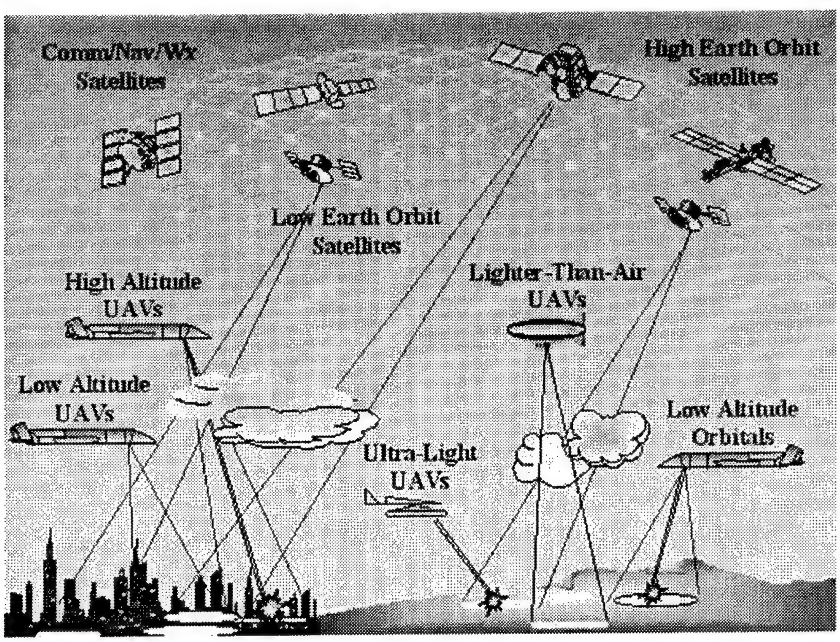



**Figure 3-6. SAF UAV "Constellation"**

concept, SAF's constellation must meet other criteria as well. The UAVs and ultra-lights must be cheap, durable—long-loiter, reliable—and create zero requirements for logistics support (i.e., cheap enough to be expendable).[30] Some of the orbitals would be camouflaged with the chameleon concept to resist detection.[31] Different configurations would answer several missions: (1) some would be configured with the LifeGuard system and potentially a delivery means for nonlethal/sublethal weapons or targeting devices; (2) others would replace EC-130 psychological operations platforms rigged with communication devices or relay antennas; and (3) certain orbitals could mimic potent lethal platforms in sound or radar cross section (e.g., the AC-130 gunship to further the deterrent ability of SAF).

Airpower's speed and maneuverability are central to neutralizing potential conflicts. Increased loiter times deliver a "psychologically exhausting presence" to coerce people to obey prevailing civil and military law or merely to instill order.[32] Introduction of pervasive UAV constellations would obviously lead to an opposing force desire to destroy or neutralize the SAF capability for political, ideological, or economic reasons. Several minimum measures would enhance constellation survivability: (1) keep it cheap—not worth killing, (2) keep it small—easy to multiply, tough to pick the "right" target, and (3) camouflage—can't see, can't kill!

**Education**

The second component of SAF's CEI is education, a long-term remedy for social or political ills. SAF constabulary forces should provide a conducive environment for education programs conducted by both local leaders and outside personnel.[33] One goal of education is to create a literate population that can support either industry or other market-friendly opportunities. Attainment of this goal would attract foreign investment as a self-fulfilling prophecy. Portions of the US education solution set can be exported via technological means to rapidly answer short-and long-term stability goals (table 5).

Today, military forces conduct traditional military-to-military education missions, primarily US Army Civil Affairs units performing civil administration and military civic action tasks.[37] However, operations in the peacespace cloud traditional roles and may cause mission creep. SAF doctrine should spell out specific military responsibilities for education and differentiate these from civilian roles and missions. Primarily,

**Table 5**

**Required Education Technology**

| MISSION | OBJECTIVE | TECHNOLOGIES OR CONCEPTS |
|---|---|---|
| Export best of US education structure philosophy,[34] & architecture, not necessarily "values" (must have broad cultural appeal) | • Initial foundation<br>• Secondary<br>• Undergrad/grad college<br>• Vocational/technical | "Selective[2] school or "dial a subject"<br>• Economics<br>• Military/Martial Arts<br>• Politics<br>• Religion |
| Global Schoolhouse[35]<br>Teach to Think & Question (not necessarily spout media sound bites) | "Tools" + Desire = Education<br>Doctrine:<br>Retain ability to read, write, and arithmetic | Brilliant Warrior[36] distance learning program basis for global schoolhouse (just as military "gave" the world Internet, we will "give" them distance learning) |
| Export hard solutions—"info" on target fixes . . . answers to natural disasters, refugees, humanitarian actions, or economic crises. | • Market/financial<br>• Infrastructure<br>Medical<br>Logistics<br>Engineering | Innovative answers for organic fixes.<br>Zero sum "imports" such as wood, water, power, food, or medicine.<br>What's here to use?<br>Come as you are peace. |

the military will continue to provide lift, information "pipes," and security for civilian or country teams.[38] The primary differences between SAF and today's forces are organization, training, and equipment tailored to the peacespace mission. SAF will allow clearly defined roles for both the nontraditional and traditional warriors in 2025.

Nongovernmental and private volunteer organizations may require airlift support of personnel and equipment. One preemptive measure of education would be to "pipe" the necessary tools and equipment remotely. Distance learning could enable foreign stability or crisis response by extensive use of communication hookups under dissimilar architecture. SAF forces could harvest innovative solutions, both military and civilian, to integrate disparate mediums and levels of technology. Print, radio, television, telephone, and computer networks all facilitate SAF missions. These lines of communications would allow passage of information, and processing or translating it, to ensure accurate comprehension and communication.

### Infrastructure

In 2025, infrastructure development will be a cooperative effort between the host nation and multinational efforts. US Commerce Secretary Ron Brown's ill-fated mission to former Yugoslavia and Croatia in 1996 was designed to bolster foreign investment in the region.[39] To achieve the desired end-state, SAF may coordinate the efforts of such agencies as the departments of Justice and State, the Environmental Protection Agency, nongovernmental organizations, multinational corporations, and private volunteer organizations for lift, security, or education. These institutions offer critical knowledge to developing a host nation's infrastructure. Those US military forces performing infrastructure missions will work side-by-side with these agencies. While SAF can build roads, bridges, and industrial facilities, and perform environmental cleanup, the bulk of infrastructure development should come from indigenous sources or foreign capital investment provided by private investors and international lending organizations.

To transition SAF out of an area or region requires a "handoff" to civilian control. Before this transition can occur, some infrastructure should be in place to entice foreign capital investment for continued economic growth. Infrastructure in this sense includes both man-made and natural elements. Stewart Brand suggests "the whole world is worried about the natural infrastructure—soils, aquifers, fishable waters, forests, biodiversity, and even the atmosphere. The natural systems are priceless in value and nearly impossible to replace, but they are cheap to maintain."[40] Table 6 outlines the projected infrastructure missions, objectives, and applicable technologies.

Infrastructure is the largest area of SAF, yet we have deliberately chosen to limit our focus to only a few examples. This area requires substantial development by experts in each field. For example, SAF may require such unique mission equipment as an autonomous cargo handling capability—essential, and achievable by advanced systems such as computer control from a cockpit console, a rapidly reconfigurable powered floor, and an articulated cargo ramp. These systems permit transfer of pallet loads directly to and from bare trucks with minimum crew member assistance.[43] Each area in infrastructure requires careful and thoughtful analysis before final planning, programming, or acquisition.

## Summary

*"Try not. Do, or Do not. There is no try."*
*"I don't believe it."*
*"That is why you fail."*[44]

While we presented many technological options to "solve" peacespace operations, the real solutions lie with people. Someone has to agree to confront peacespace problems. We believe that person should be

**Table 6**

**Required Infrastructure Technology**

| MISSION | OBJECTIVE | | TECHNOLOGY | |
|---|---|---|---|---|
| Category | SAF rqmts | Customer rqmts | SAF rqmts | Customer rqmts |
| Acquisiton | Specialize in acquisition of non or sublethal wpns | Exploit organic capability through contractual actions before "importing" Western goods or services | N/A | Situation dependent |
| Logistics<br>• Supply<br>• Maintenance<br>• Transportation<br>• Plans | Primarily commercial off-the-shelf or contracted support | Situation dependent<br>• Food, water, shelter?<br>• Industrial?<br>• Advanced technical? | Situation dependent | Situation dependent |
| Medical | • Preventive care[41]<br>• Triage (SAR)<br>• Medevac | • Organic capability<br>• Preventive care<br>• Triage<br>• Advanced care<br>• Infrastructure | Tailored to environment | Tailored to long/short-term needs |
| Personnel | • Small, rugged, mobile<br>• Selected for behavior traits | N/A | Increase intel dependence—keeps force small | N/A |
| Training | • Restraint<br>• Conflict prevention<br>• Conflict resolution | Tailored to region | Unlimited potential | "Global schoolhouse" |
| Engineering | • Power, roads<br>• Billets | • Power, roads, rail<br>• Buildings | Reusable buildings[42] | • expertise<br>• organic |
| Command, control, communications, computers | Service and commercial dependent | Depends on level of development & cultural needs | Robust and minimum architecture | Lend/lease commercial enterprise |

a warrior, not a wizard. Defining Liddell Hart's "better state of peace" may reveal exactly why we choose to engage. We *may* opt to apply SAF's force, avoid the battle, and enter the peacespace for prevention or resolution. Accepting the challenge to shape the better state of peace determines the rules and tools.

SAF's constabulary, education, and infrastructure force is evolving even now. Many traditional military tasks are migrating to civilian contract or civil service. Nongovernmental and private volunteer organizations are proliferating as quickly as web sites on the Internet. These questions must be addressed. The US military option for maintaining credibility, legitimacy, and competency as warriors may be as simple as leading the way. SAF is one answer to this problem.

### Notes

1. Liddell Hart, *Strategy* (1954; new imprint, New York: Meridian, 1991), 338; Fred Charles Ikle, *Every War Must End* (New York: Columbia University Press, 1991), 106–31; Paul Seabury and Angelo Codevilla, *War, Ends & Means* (New York: Basic Books Inc., 1989), 263–69. Liddell Hart, Ikle, Seabury and Codevilla developed a fascinating thesis through the past 42 years. Liddell Hart began with a simple but ill-defined sound bite, "better state of peace." Ikle discusses ending wars before they begin. Finally, Seabury and Codevilla distill the argument down to three choices: (1) peace of the dead, (2) peace of the prison, or (3) peace by cultural conquest. Dr Cable ("The End-State," lecture, 16 January 1996), contends the "dead dictate policy" for any nation bringing conflict to closure. Obviously, the notion of *peace* consumes the intellectual and military alike. Our most fragile

problem today remains—deciding exactly what a better state of peace means to ourselves and our opponents.

2. The digital cultural map depicted and envisioned would be a complex beast (i.e., an equivalent supercomputer in 30 years) that ties into a nearly unlimited number of open source databases and archives. Several examples would include weather, financial, agricultural, cultural (religious, language and dialects, ethnic), population, disease, technological advancement, infrastructure, water or food source and supply. Leaders could select specific geopolitical or geostrategic map displays. Tripwires and flashpoints for intervention could be triggered through a combination of the fuzzy cognitive mapping technique described by Bart Kosko, *Fuzzy Thinking, The New Science of Fuzzy Logic* (New York: Hyperion, 1993), 222–32; and Maj Glenn James, "Chaos & Campaign Planning," lecture, Air Command and Staff College, Maxwell AFB, Ala., 8 March 1996. The database management and weighting of individual intangibles would remain largely the purview of cabinet level staffs. Ultimately, a leader could peel back the layers of the onion on demand to review migratory trends or consumption data, or to evaluate measures of effectiveness for investments made. This concept would rely on unprecedented interagency, international, and individual cooperation.

3. Alvin Toffler and Heidi Toffler, *War and Anti-War* (New York: Warner Books, 1995).

4. Benjamin Schwarz, "The Diversity Myth: America's Leading Export," *The Atlantic Monthly* 273, no. 5 (May 1993): 67. Schwarz asserts US intervention in ethnic, nationalist, and separatist (ENS) wars should be an option only when specific, vital US interests are threatened."

5. This doctrine section adapts original tenets of aerospace power as listed in AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol 1, March 1992, 8. Also, Col Phillip Meilinger, USAF, wrote a treatise, "10 Propositions Regarding Air Power," Air Force History and Museums Program, February 1995. Proposition 5 states, "Air Power produces physical and psychological shock by dominating the fourth dimension—time." This proposition led Colonel Meilinger to conclude: "This leads to an important insight regarding the effectiveness of airpower in low-intensity conflicts. Because guerrilla war is protracted war, by its very nature it is ill-suited for air power, denying it the ability to achieve decision quickly." This conclusion ignores the potential for airpower as demonstrated by the Navy in Bosnia and likelihood of UAV, UCAV employment. Col Richard Szafranski rebutted Colonel Meilinger's position in "Twelve Principles Emerging from 10 Propositions," *Airpower Journal* 10, no. 1 (Spring 1996): 51–80. Certainly all land, air, and sea dominance missions, either civilian or military, require disciplined examination of preconceived notions in the "new world order." This paper only addresses some air disciplines involved. We recommend the reader search such lucrative sources as Toffler and Toffler, *War and Anti-War*, 19–27, 103–13, 146–57; Thomas J. Peters and Robert H. Waterman, Jr, *In Search of Excellence* (New York: Warner Books, 1982), 89–119; Michael Hammer and James Champy, *Reengineering the Corporation* (New York: Harper Business, 1993), 31–50. SAF will require innovative doctrine that synthesizes military and civilian philosophy into a single, seamless structure. For example, Toffler and Peters provide examples from the civilian world which would enrich military doctrine.

6. Toffler, 67–68.

7. UAVs and long-loiter platforms provide the ultimate in persistence. As technology improves, they give many of the advantages of physical presence without the disadvantages. Thus airpower is found in many venues such as the recent employment of the Predator UAV off the *USS Carl Vinson*. In the extreme case, you would pursue some goals without ever physically occupying the land. The current debate over "air occupation" notwithstanding, sufficient "air dominance" should significantly reduce the number of ground personnel required as well as decreasing the risk of casualties. Additionally, Dr Larry Cable (interview with authors, 28 March 1996) notes that "physically exhaustive presence" often succeeds in wearing down the will to resist and airpower is uniquely suitable to this task.

8. Composite force doctrine is fertile ground for further research and inquiry. Peacespace forces require the discipline of other fields such as international organizations, politico-economic analysis, crisis resolution, and comparative politics. Lt Col Ann E. Story and Major Aryea Gottlieb call for additional work in their article "Beyond the Range of Military Operations," *Joint Force Quarterly*, Autumn 1995, 99.

9. We have included a list (appendix B) of all technologies for ease of reference.

10. We arrived at these force structure characteristics after careful investigations of current efforts around the world by US military personnel. While one senior officer agreed "4000 was about right (brigade size)," he did not advocate the conversion of any combat forces to this role. Zero sum budgets artificially constrain speculation of possibilities for 2025 force structure changes. Also, military personnel are covered by "limited" liability and have the right to die for their country without recourse (Feres Doctrine). Force structure for civilian expertise requirements in hazardous, albeit peacespace conditions, and their implications are not addressed in this white paper.

11. Carl H. Builder, "Doctrinal Frontiers," *Airpower Journal* 9, no. 4 (Winter 1995): 9.

12. Maj Edward O'Connell, USAF, "Nonlethal Concepts: Implications for Air Force Intelligence," *Airpower Journal* 8, no. 4 (Winter 1994): 26–33. In his first draft of this article, Major O'Connell developed a concept for a mixed-bag adaptive response capability where both lethals and nonlethals are configured aboard a B-1 aircraft. With advanced command and control capability, NCA could redirect responses in

flight as the ground situation changes from "hot" to "cold." He was instructed to remove this section before publication. Used by permission.

13. Col John Warden, *The Air Campaign: Planning for Combat* (Washington, D.C.: NDU Press, 1988), 4. Colonel Warden introduces a concept for battlespace dominance now known as "strategic paralysis." Peacespace dominance may need a "strategic paralysis" to impose the pause required for a change of course or course correction.

14. We have only begun the transition to less than lethal technology and now that change will affect the way we execute the business of war. The impact will probably be immense. Suggest reading Capt Vicki J. Rast and Maj Bruce R. Sturk, "Coalitions: The Challenge of Effective Command and Control in Support of the Air Campaign," *Air Command and Staff College Theater Air Campaign Studies Coursebook* (Maxwell AFB, Ala., 1996), 169–90. Rast and Sturk provide an excellent analysis of direct and indirect effects versus effectiveness, and the often hidden second-order consequences for actions taken during any campaign. Second-order consequences are effects felt "down the road" and not readily apparent at the time. This paper is a necessary read for anyone establishing the SAF concept.

15. ***2025*** Concept, no. 900664, "Tiltwing Super Short Take off and Landing Advanced Theater Transport," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); ***2025*** Concept, no. 900203; "Heavy Lift Aircraft with Mission Pod," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the mobility volume, 15 December 1995), 15, 16, 22; "New World Vistas" (unpublished draft, the aircraft and propulsion volume), 39; ***2025*** Concept, no. 900906; "Personal Identification Friend or Foe (PIFF)," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

16. Calmative agents are but one category of an ever-increasing litany of nonlethal weapons.

17. During the team brief to HQ AFSOC/CV on 6 March 1996, Brig Gen Ingersoll discussed the requirement for vertical emplacement of water purification devices. In 1996, this requires the cubic space of a C-5, a significant shortfall in current lift capability.

18. Szafranski, 76. Colonel Szafranski notes the greatest weakness of airpower lies in the fact we "can blow a door off of its hinges, but—unlike a simple soldier or marine—airpower cannot see what is behind the door."

19. Toffler and Toffler, 185.

20. Ibid.

21. Ibid., 186, 189–90. One example of "innovative" intelligence gathering would have been monitoring how long before the invasion of Kuwait Lloyds of London stopped issuing insurance in the region.

22. "New World Vistas" (unpublished draft, the aircraft and propulsion volume), 10, 43; ***2025*** Concept, no. 900701, "Long Duration UAVs," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); ***2025*** Concept, no. 900763, "Unmanned Mini Helos," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); "New World Vistas" (unpublished draft, the sensors volume), 48, 50, 57, 62; "New World Vistas" (unpublished draft, the directed energy volume), 29.

23. Colonel Szafranski coined this phrase in a paper co-authored with Dr Martin Libicki entitled, ". . . Or Go Down in Flame: An Airpower Manifesto for the 21st Century," unpublished ***2025*** white paper. Used by permission.

24. Figure 3-4 in the air dominance section depicts the envisioned UAV Constellation including both air occupation platforms and ISR/$C^4$ orbitals.

25. See Szafranski, "Twelve Propositions," 73, for a caveat. We present air dominance as one possibility to reducing the total ground troops required, not necessarily to replace them entirely.

26. Builder, 11–13.

27. Not all of the constabulary missions are "high tech." Cable's "psychologically exhausting presence" may encompass "low tech" alternatives which were successfully employed in Just Cause and other special operations/conventional missions. Some examples of "low tech" would be lights, lasers, noise, and "positive" communication. Scott R. Gourley, "The Sniper's Latest Nightmare," *International Defense Review* 28, no. 4 (April 1995): 66. Gourley reports on the Lawrence Livermore laboratory concept for computerized thermal bullet-tracking capability developed by Dr Thomas Karr and originally brought to our attention by Janet Morris. Further investigation revealed Bosnia officials requested this technology as part of their containment efforts. (Also in *Wired* magazine, *Newsweek*, and *Washington Post*.) Hereafter referred to as LLLab concept. ***2025*** Concept, no. 900705, "Anti-Sniper Probability Device," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); "New World Vistas" (unpublished draft, the attack volume), 11, 13; "New World Vistas" (unpublished draft, the directed energy volume), 9; ***2025*** Concept, no. 900658, "Urban Assault Helo Vehicle Hybrid," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); "New World Vistas" (unpublished draft, the aircraft and propulsion volume), 10, 24; ***2025*** Concept, no. 900711, "Multipurpose UAV," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); ***2025*** Concept, no. 200009, "Pyrotechnic Electromagnetic Pulse 'PEP'," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); ***2025*** Concept, no. 900699, "Chameleon Camouflage," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996); ***2025*** Concept, no. 900753, "Full Body Armor," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

28. LLLab concept.

29. "Constellations" will encompass a complex architecture by 2025, composed of low-altitude (atmospheric or air breathing) orbitals, low-earth orbitals, and so forth. Just as gunships, tankers, and AWACS "orbit" in racetrack patterns in 1996, new UAV replacements would employ these and new tactics.

30. Lean logistics, two-level maintenance, and streamlined acquisition process concepts currently allow circuit cards valued from $3,000 to $33,000 to be disposed without developing technical orders, test stations, or training for their repair. This trend, coupled with industry's response for "just in time" supplies, may change our preconceived notions of what is expendable and what should be repaired. This same logic applies to the automobile industry—we "replace" computers instead of "repairing" the old Chevy.

31. ***2025*** Concept, no. 900699, "Chameleon Camouflage," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

32. Cable, "The Dangers of Dogma," lecture, Air Command and Staff, Maxwell AFB, Ala., 28 March 1996.

33. Lt Col Federico J. Rodriguez, PhD, USAR, "Interdisciplinary Collaboration in the Americas," *The Officer* 62, no. 3 Reserve Officer's Association of the US (March 1996): 24–27. Dr Rodriguez is the professor of graduate education at California State University, Dominguez Hills, California. The Collaborative Educational Programs for the Americas (CEPA) is an international program that brings together an interdisciplinary group of professionals from education, law enforcement, and the military to meet future challenges and to develop an educational infrastructure for personnel and material resources. "This program serves as a model for education and social reform within our [southern] hemisphere for the 21st century." Rodriguez' insight and suggestions were invaluable to our research efforts.

34. Lt Col Anita M. Arms, "Strategic Culture: The American Mind," *ACSC Theater Air Campaign Studies Coursebook*, 1996, 150–63. In a subsection of this article, Ms Arms discusses education as the equalizer in "purveying political ideology to immigrants and native-born (Americans) alike. Further, in an endnote, she quotes Michael Olneck and Marvin Lazerson, "Education," *Harvard Encyclopedia of American Ethnic Groups*, Stephen Thernstrom, ed, 304. It is also interesting to note the lack of a national school system effectively prevented, and still prevents, arbitrary testing that would divide students into white collar and blue collar educational tracks early. University attendance still does not depend on the score of an exam taken at age 10 or 12. It depends on completing high school with grades high enough to meet the college entrance requirements. It permits the illusion that in the US, anyone can succeed, and thus furthers the belief in social equality.

35. Schwartz, *The Art Of the Long View*, 125. Schwartz discusses at length the possibilities associated with technology and education in the future, especially as associated with the "Global Teenager."

36. Lt Gen Jay Kelley, Air University commander, "Brilliant Warrior," ***2025*** white paper (draft).

37. Joint Publication 3-0, *Doctrine for Joint Operations*, 1 February 1995, v-1 through vi-12.

38. Dr Martin Libicki, "Battlespace Dominance," lecture, 25 March 1996. Dr Libicki briefed the evolution of communications "pipes" which carry data such as telephone lines, television cable lines, and power lines. The size restricts the throughput and is the next step in the information "revolution."

39. Bill Montague and Christine Dugas, "Peacemakers Slow to Invest in Bosnia," *Pensacola News Journal*, Gannett News Service, Sunday, 7 April 1996, 3D. US companies invested $4.5 million in Croatia from 1992 to 1994 representing just 4.4 percent of foreign investment. The World Bank approved $269 million in loans for three projects on 1 April 1996. The US and other nations have promised to fund a $5.1 billion plan to rebuild bridges and other infrastructure.

40. Stewart Brand, "Army Green." Document was originally published in *Whole Earth Review*, Issue #76; on-line, Internet, 14 May 1996, available from gopher://gopher.well.sf.ca.us:70/00/WER/Army/Green.

41. We envision development of a computerized personal doctor that maintains individual history, takes vitals, and emits basic prescription requirements which is "licensed" to practice medicine for deployed troops.

42. On 10 April 1996, 2100 hours, Montgomery Alabama Public Broadcasting Channel (PBC) ran a special on Buckminster Fuller, an engineer who developed geodesic structural designs in the 1950s. Shunned by the architectural community as little value added, these structures have greater tensile strength than "stick-built" homes, they snap up and down relatively quickly, and can be stored until required. "Architect, inventor, scientist, teacher and philosopher, he advocated intelligent use of the earth's resources to gain the maximum return for the minimum of material and energy expended, and produced numerous models of how it could be done." Information provided by Lt Comdr Alton Ross, Air Command and Staff College, Seminar 17, 1996. On-line, Internet, 14 May 1996, available from http://www.echonyc.com/~mysticfire/MABucky.html.

43. ***2025*** Concept, no. 900664, "Tiltwing Super Short T/O and Landing," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996). Also articulated by General Ingersoll as a dynamic factor in current operations.

44. Yoda speaking with Luke, *The Empire Strikes Back, ©1980, Lucasfilms Ltd.*

## Chapter 4

# Concept of Operations

*It's not the bullet with my name on it that worries me. It's the one that says "To whom it may concern."*

—Anonymous Belfast resident

With clear entry criteria, SAF conducts its operation. Three notional scenarios illustrate our concept. To combat a cholera outbreak in Benin caused by contaminated water, SAF would deploy directly into outbreak areas in strategic aircraft using advanced navigation systems coupled with vertical take-off and landing platforms. Simultaneously, containerized inoculation facilities and medical teams would deploy to remote regions and provide medical care. In this instance, levels of violence are low, thus reducing the need for a SAF constabulary force. SAF's primary role would be to contain the disease outbreak and prevent further occurrences. Long-term fixes result from educating the population on health and sanitation procedures. The primary education effort would be civilian-led with SAF assistance, protection, and delivery. SAF would only minimally improve Benin's modest infrastructure. The SAF military effort would be short-term (less than one year) with follow-on education and infrastructure terminated in the midterm (five years).

In another scenario, a region is in a state of anarchy, suffering from a collapse of its infrastructure. This region is marked by widespread disease and mass famine—similar to the situation US forces encountered in Somalia. In this scenario, US/UN conventional forces would first move to secure the area. SAF units would then deploy in-country via strategic lift, reducing the need to maintain security of port facilities. In their constabulary role, SAF would employ both nonlethal weapons and linguists to develop and maintain order. Constabulary forces could establish judicial processes, local police, and legal institutions to permit an effective transfer of law and order duties to local authorities.[1] Constabulary forces would also employ ultralight UAV to ensure air dominance and provide continuous presence while reducing risks for ground force elements. Technology such as LifeGuard would identify snipers and other potential combatants. Simultaneously, education and infrastructure personnel would provide medical and famine relief. In this example, the constabulary effort to redress violence is modest. Education requirements are high as they must effectively "jump start" and sustain sufficient infrastructure development to maintain a better state of peace. This would be a mid-term effort—five to 10 years.

Finally, factions may actively fight in a technologically adept society similar to those of the former Yugoslavia or Northern Ireland. If leaders decided to intervene, special or conventional forces may engage the combatants before SAF would assume their constabulary role. Constabulary duties could be long-term (greater than ten years), pending a political settlement (as in Northern Ireland). Traditional education efforts would be minimal if key indicators (such as literacy rates) are high. Infrastructure needs would be both high and long-term if the infrastructure suffers widespread destruction (as in former Yugoslavia). Infrastructure rebuilding could be accomplished in five to 10 years. If leaders decide to progress a first wave society to the second or third wave, SAF would require a 20 to 30-year commitment.[2]

Some scenarios will remain beyond SAF's core competencies. Conflicts based on deep-seated cultural or political differences will likely have to be solved at the bargaining table before SAF's introduction. SAF constabulary forces could separate belligerents (at great risk), but centuries old hostility and a nearly unlimited willingness on the part of some factions to kill one another may exceed all available resources. New options and solutions such as non-lethal weapons, advanced airlift, cultural knowledge, funding, or even improved infrastructure may prove fruitless. However, a preponderance of missions tackled in 1996 fall neatly into SAF's area of expertise.

**Notes**

1. Discussions with Headquarters Air Force Special Operations Command personnel who participated in Operation Just Cause revealed the methods for transfer of law and order responsibility from military to civilian personnel. Essentially, Panamanian Defense Force (PDF) personnel were offered asylum and amnesty in exchange for turning in their weapons. At the first station, PDF members would relinquish their weapons. At subsequent stations, they would (1) denounce the current regime, (2) indicate a desire to serve under the new regime (3) swear allegiance to the new regime, and (4) receive back their weapon and a schedule for training and indoctrination.

2. Alvin Toffler and Heidi Toffler, *War and Anti-War* (1993; new imprint, New York: Warner Books, May 1995), 35–94.

# Chapter 5

# Recommendation

*Frankly, I'd like to see the government get out of war altogether and leave the whole field to private industry.*

—Joseph Heller

This paper asserts the need for a force dedicated to preventing conflict. On 13 May 1996, Secretary of Defense Perry stated, "America must lead the world in preventing the conditions for conflict and in creating the conditions for peace. In short, we must lead with a policy of preventive defense. It's about hard work and ingenuity today, so that we don't have to expend blood and treasure tomorrow."[1] In this chapter, we will discuss plausible options for implementing SAF—a blueprint for change.

One option encompasses either unilateral US action or a US-led multinational team in performing the SAF mission. This option has several merits, since it avoids placing American lives in the hands of others and allows the US to determine its own destiny. In addition, the US possesses unique capabilities that argue for its leadership: we have enormous energy, and we often lead in managerial and technological initiative; harnessing the power required to avert war is within our capability; and leading the SAF effort will foster the perception that we are "giving back" to the rest of the world in some tangible way.

The US role as lead agent could have unintended consequences. US efforts might be caricatured as a latter day "white man's burden," where we solve the world's problems by exporting US values and beliefs. This would be unpalatable in many cultures. Also, the temptation exists for the US to favor our interests at the expense of the resident population. This is not only bad public relations, it is also counterproductive to US interests in the long run.

It may also be in US interest to allow an "evolved" UN—or another nation—to lead in developing a SAF capability. Peacespace dominance may be more suitable for other nations (Japan, Singapore, Scandinavian countries, Canada) which have forsworn the use of force or are perceived as more neutral. Their domestic cultures might be more conducive to performing a SAF role.

The drawbacks to this option: The US may have little leverage determining if and when an intervention should be made; we can exercise little control once the mission starts; and these operations require substantial funding. Would the US be willing to pay when we are not "calling the shots"?

Another option may be to stay the course. It can be argued that the current system is working fine and needs only minor modifications to the concept of operations and to doctrine.[2] Many assert that the military can both keep the peace and fight. In their view, ramping down for peace operations is well within the present capability of the military. Our warriors are well-educated, trained, and psychologically nimble enough to do both.

This is not a universally-held view however. Opponents argue that SAF would free the conventional military to concentrate on its primary combat mission while providing a critical capability in crises that will only become more numerous and complex. Table 7 summarizes three possibilities for peacespace dominance.

**Table 7**

**Responsibility for SAF**

| | US Unilateral or US Led Multi-National | UN Initiative or "other National" Effort | Stay the Course |
|---|---|---|---|
| **Pros** | • US leadership prods other nations to act<br>• Education structure and technological prowess ("science" skills) enjoy a reputation as "best" in much of the globe<br>• Education is a great export item<br>• World's largest economy, highest per capita income, and low debt as percentage of gross domestic produce = we pay for "it," therefore we should *do* it<br>• Improved public image for sharing the wealth | • Nations who have forsworn the use of armed force possess instant creditibility abroad<br>• Already perceived as neutral<br>• Cultures are amenable to the concept<br>• Other cultures' education systems are already sophisticated in art of conflict resolution and prevention as opposed to simply termination | • Military easily ramps down from combat mission<br>• Current system largely works with minor doctrine/training modifications |
| **Cons** | • unintended consequences<br>• makes US a target rather than a benefactor ("I'll help as long as you do it *my* way")<br>• US lead or unilateral action creates obstacles obtaining "legitimacy" . . . might be viewed as imperialistic | • Legitimacy of UN interventionary action is currently questionable<br>• US interests may diverge from UN<br>• Entry/exit criteria blur for UN | • The system is broken and should be fixed<br>• Performing *peacespace* missions erodes combat capability |

## Conclusion

What needs to be done to make SAF a reality? This paper only touches areas which beg greater exploration.[3] Leaders have 30 years to focus energy and funds against specific requirements and capitalize on existing progress. Joint, service, and civilian doctrine need to apply rich lessons learned from the past. The technologies mentioned in this paper hint at the possibilities.[4] The digital cultural map might accurately predict and identify trouble areas, but the concept requires careful study prior to development. Unmanned aerial vehicles, nonlethal weapons, and a "global schoolhouse"—all present tantalizing possibilities.

Like US businesses struggling to restructure, the US military has transformed itself from the demoralization of the 1970s to a peak performer in 1990—"an elegant force."[5] An evolving world order, increasing demands on declining resources, and potential technologies afford the "elegant" warrior an unprecedented opportunity. If properly developed, planned, and funded, SAF could be available in 2025 to help dampen violence and orchestrate the peace. The military has demonstrated an ability to lead the way and change the future. It is in our best interests to act.

What vast additions to the conveniences and comforts of living might mankind have acquired, if the money spent in wars had been employed in works of public utility; what an extension of agriculture even to the tops of our mountains; what rivers rendered navigable, or joined by canals; what bridges, aqueducts, new roads, and other public works, edifices, and improvements . . . might not have been obtained by spending those millions in doing good, which in the last war have been spent in doing mischief.[6]

### Notes

1. William J. Perry, remarks delivered to the John F. Kennedy School of Government, Harvard University, on-line, Internet, 13 May 1996, available from http://www.dtic.mil/ defenselink.

2. Col Anthony Wood, USMC, Quantico Warfighting Laboratory Director, "Sea Dragon: Warfighting in the

Future," lecture, Air War College, Maxwell AFB, Ala.: 17 May 1996. Colonel Wood stated a corollary to the familiar maxim "If it ain't broke, don't fix it," which says "Just cuz it ain't broke, don't make it relevant."

3. "World View: The 1996 Strategic Assessment from the Strategic Studies Institute," ed. Earl H. Tilford, Jr., (Carlisle Barracks, Pa.: US Army War College, 1996), 12. Steven Metz eloquently summarizes the requirement to explore these questions in depth. Most importantly, Tilford concludes on page 54, "If the Army is to have the capabilities to deter and, when necessary, to compel calculating aggressors of this nature, it must be able to resolve conflicts at levels where human and economic costs are sufficiently low to justify intervention. Otherwise, extortion of the Army's ability to promote and protect nonvital interests will result.

4. Maj Kenneth E. McKenzie, Jr., USMC, "An Ecstasy of Fumbling: Doctrine and Innovation," *Joint Force Quarterly*, Winter 1995–1996, 67–68.

5. Kevin Kelly, "Shock Wave (Anti-) Warrior," *Wired*, February 1995; on-line, Internet, 14 May 1996, available from: http://www.hotwired.com/wired/1.5/features/toffler.html. The US military has "gone from the pits of post-Vietnam, drug-drenched, corrupt, bloated bureaucracy into an elegant force." Alvin Toffler in conversation with Peter Schwartz as reported by Kevin Kelly.

6. Benjamin Franklin (1706–90), US statesman, writer. Letter, 27 July 1783, to Sir Joseph Banks, president of the Royal Society, after the American War of Independence (published in *Complete Works*, vol. 8, ed. by John Bigelow, 1887–88). *The Columbia Dictionary of Quotations*, (Columbia University Press, New York: Copyright © 1993). Microsoft ® Bookshelf.

# Appendix A
# Criteria for Intervention

| CATEGORY | CRITERIA | METRIC* |
|---|---|---|
| Sociopolitical | Education literacy rates | percent increase |
| Sociopolitical | Education infrastructure | growth in secondary, vocational technical schools, colleges, university-type institutions |
| Sociopolitical | population growth or birth rates | deviation from what region can organically support |
| Sociopolitical | multilateral intervention requested | existence of coalition, status of forces, or treaty agreement |
| Sociopolitical | universal suffrage | laws passed/polls measure *(cannot be unilaterally applied vis-á-vis Muslim nations)* |
| Sociopolitical | liberties/human rights | international measurement |
| Sociopolitical | environmental consumption | conservation technology |
| Infrastructure | indigenous medical capability | rates of infectious disease, infant mortality |
| Infrastructure | transportation network | adequacy of roads/ports/airfields to meet "universal" standards |
| Infrastructure | power grid | ability to convert/upgrade to "universal" standards |
| Infrastructure | communication grid | ability to convert/adapt to "universal" standards *(required/desired?)* |
| Infrastructure | agriculture base | ability to feed population |
| Infrastructure | potable water supply | adequate to consumption and sufficient for expected growth |
| Infrastructure | industrial capacity | as required |
| Economic | knowledge base | exportable? perceived value? |
| Economic | market structure<br>import/export rates | open/closed<br>MFN status |
| Economic | employment rates | percent improvement . . . appropriate to 1st, 2d, 3d wave |
| Economic | inflation rate | control mechanisms |
| Economic | GDP/capital spending/interest rates | "stability" or growth indicators |
| Economic | per capita income/personal income | relative personal expectations |
| Financial | existing internationally recognized "institutions" | adaptability to universal standards of financial trade (i.e., convertible currency/foreign exchange rates) |

* As per Dr Martin Libicki and others, to quantify costs leads to "Slighting the Intangibles" or excessively weighting the analytical vice versa intuition. SAF needs balance. Such tools as a digital cultural map, using fuzzy cognitive mapping (Bart Kosko, *Fuzzy Thinking*) or chaos theory (Maj James lecture) should help to qualify, not quantify.

# Appendix B
# Underlying Technologies

Technology concepts from the USAF Scientific Advisory Board's (SAB) *New World Vistas* and technology concepts submitted for the 2025 study were reviewed for applicability to the SAF. Concepts harvested from these efforts, which directly or indirectly apply to the SAF roles of constabulary, education, or infrastructure, are summarized and included below.

## Aircraft and Propulsion Volume

**Uninhabited Aircraft or Unmanned Tactical Aircraft (UTA).** This concept would develop unmanned aerial vehicles (UAV) to do the air-to-air, suppression of enemy air defense (SEAD), strike, and surveillance & reconnaissance (S&R) missions currently done by manned aircraft. The concept also envisions that, without a human in the aircraft, the vehicle could be miniaturized to reduce signature. These UAV could provide some of the ISR, SAF needs to conduct an air occupation.

**Modular Vehicles.** This concept calls for manufacturing aircraft that are modular in their components and use. The concept would permit a force to mix-and-match "parts" of an aircraft to change its role. Modular parts would also aid in maintenance. Instead of fixing an engine in the field, the team would simply replace the engine module with a new one. The concept would reduce the logistic tail brought into the field by SAF.

**Future Attack Aircraft.** This concept envisions a 500-nm-range manned or unmanned aircraft that would use stealth technology (both RF and IR) to reach a target and employ laser or high-power microwave (HPM) weapons. An unmanned aircraft with a "tunable" HPM weapon could provide either the nonlethal or lethal punch SAF needs in the constabulary mission.

**Special Operation Forces Vehicle.** This 1500-nm radius, high subsonic speed, vertical take-off and landing (VTOL) aircraft would employ low-observable (LO) technology to reduce signature. The concept is evolutionary and would represent the next generation V-22. This concept could provide the tactical transport for SAF and the primary search and rescue vehicle to recover SAF personnel in distress.

**Long-Endurance Aircraft.** The concept envisions an unmanned aircraft that can fly for days, weeks, even months, at an altitude of 80,000 feet or more. This high-altitude, long-endurance (HALE) aircraft, with an appropriate suite of sensors, could provide the constant monitoring platform SAF needs. The engines would be solar-powered props, and the aircraft could carry a 2,000-pound payload, enough for sensors or even a single weapon. One drawback for such an aircraft is that its wingspan would probably require it to self-deploy, which might take days.

## Attack Volume

**Radio Frequency (RF) Warhead, Disabling Enemy RF Sensors.** This concept would use UAVs to get very close to the enemy and emit a pulsed RF transmission to knock out the RF (radar, communications) equipment of the enemy. The concept would provide a nonlethal weapon for SAF to use on modern weapons.

**Suppress Hostile Artillery.** Using moving target indicators (MTI) on UAVs along with unmanned ground sensors (UGS, see later), the concept could track the location of firing artillery and then react with a killer UTA. Expanding on this concept, if SAF were to use multiple UGS sensors along with very accurate MTI sensors on a UAV, we might be able to track sniper rounds over a large area. Once a "shooter" is detected, the UAV could employ lethal or nonlethal weapons.

## Directed Energy Volume

**Laser Power Beaming.** The concept would provide energy (power) to remote systems. For example, this ground laser could "shoot" at a receiver on an orbiting satellite to reenergize it. The laser would work for any electrically powered system.

**Virtual Presence.** The concept would use a laser to "scan" an area to provide a picture of the area the laser strikes. If combined with in-orbit mirrors, US leaders could obtain real-time pictures of any location in the world. Potentially, the laser could be used like a fiber-optic cable to shine anywhere in the world. The presentation would resemble a TV picture of where the laser hits solid mass. This concept would help SAF monitor situations as they develop and could help in determining if SAF should be employed in an area before we place personnel on the ground.

## Mobility Volume

**Global Range Transport.** This concept would provide an aircraft with a 12,000-nm range and a 150,000-pound payload capacity. The aircraft would require a runway to land, but the concept could employ the precision airdrop concept.

**Global Navigation System.** This concept is an evolution of the current Global Positioning System (GPS). Improved sensors, coverage, and receivers could increase navigation accuracy to one meter.

**Advanced Material Handling Equipment.** The concept would provide a solution for how to load or unload cargo from an aircraft when aerial port equipment is not available. One potential technological solution is to load cargo on magnetic levitation pallets. At the destination, the pallets would levitate from the aircraft to where the payload is needed on the field. This concept would be very useful in reducing the amount of equipment SAF would need at a field before moving into the area.

**Precision/Large-Scale Airdrop.** Using GPS for positioning and light-or laser-imaging detection and ranging (LIDAR) to determine winds, cargo could be dropped into a small area. Though not mentioned in the volume, if we take this concept and add the use of pallets with remote or automatically controlled fins, wings, or stabilizers, and steerable (square) parachutes, we could steer the pallet to exactly where it is needed, maybe within a couple of meters. This hybrid concept would basically give a form of precision-guided cargo (PGC).

## Sensor Volume

**Target Reporter.** The concept involves fielding a UAV with a 72-hour endurance, 4,000-pound payload, and a normal operating altitude of 65,000 feet that could hold various sensors to cover a 200 x 400-nm area. Sensors include

electromagnetic spectrum measures (ESM), moving target indicators (MTI), synthetic aperture radar (SAR), and receivers for UGSs. Data from the ESM, MTI, SAR, and UGS sensors would be fed into an auto target recognition (ATR) system that would classify each target and report the data. This system (a UAV with multispectral sensors) would meet the intelligence, surveillance, and reconnaissance needs of SAF.

**Unmanned Ground Sensors.** An acoustic UGS was used along the Ho Chi Minh trail during the Vietnam War. Modern UGSs could sense acoustic, seismic, chemical/biological, ESM, or magnetic emissions. Many of these systems placed over an area could be used to report activities. Data could be relayed to a UAV overhead (such as the target reporter concept) or, if a small and powerful enough energy source could be developed and installed in the UGS, the UGS might be able to report directly to a satellite.

**Weather Surveillance and Prediction.** Using a UAV with passive infrared, passive microwave, LIDAR, and Radar systems, enough information can be gathered to report the weather and to make reasonable predictions. This valuable information would be used in the initial deployment of SAF teams.

**Low-Cost Space-Based Surveillance.** The concept envisions multiple low-cost ($25M in FY95 dollars) satellites. The low cost is due to the limited life of these satellites—approximately six months. The systems could be tailored to the need of the customer and launched on demand. In the long run, it might cost much less to place as many as 10 of these satellites to get high coverage over an area (especially during the initial constabulary phase of a SAF operation) than it would cost to move (and use the limited life of) a $500–$700M satellite.

## *2025* Study

### Pyrotechnic Electromagnetic Pulse (PEP)

Concept no. 200009 would use pyrotechnic explosions to produce electromagnetic pulse (EMP) radiation to affect enemy sensors and communication equipment. SAF could employ weapons with small versions of this explosive to reduce the ability of organizations to coordinate their actions.

### Noise

Concept no. 900153 is a hand-held, directed, variable-pulse noise weapon that could be capable of a range of options from disorienting to incapacitating the enemy. A larger, directed-noise weapon could be used to attack larger targets ranging from mobile launching systems to military infrastructure. These weapons could easily be mounted on land vehicles or satellites.

### Mission Pods

Concept no. 900203 is the development of mission pods that could be quickly loaded and unloaded from a transport aircraft. Once deployed at its location, a pod would provide all essentials (e.g., power, lighting, computer, and communication equipment). Medical, command and control, teaching, UAV control, and water treatment pods could be developed.

**Inflatable Workspace**

Concept no. 900255 is containerized, modular, and state-of-the-art buildings that could be deployed to provide workspace for SAF teams. For more transitory encampments, huge tents that inflate from relatively small packages could be used. Several tents could be tied together or, technology permitting, tents the size of shopping malls (from individual packages fitting in the cargo compartment of a heavy-lift vehicle) could be developed. An instantly inflatable tent would decrease setup time and alleviate on-site requirements for deployed SAF teams.

**Force Sustainment**

Concept no. 900433 is a pill, shot, or internally-planted nutrient that provides all the necessary nutrition for an individual in combat for up to seven days. It would be chemically controlled to provide required nutrients over the stated period. It would not eliminate the need for water. It would be most useful for personnel in transit or in sustained conflict prevention. The pill or shot would have minimal short-term effect on the digestive system. Compounds could be included that would reduce the urge to eat. This would be a "sensitive" way to sustain forces in famine areas.

**Steerable Pallets**

Concept no. 900485 is to airdrop loads with steerable chutes, controlled by a computerized navigation system, on any desired drop zone (DZ). Loads could find the DZ via differential GPS. Steerable loads could compensate for unknown winds and give unprecedented accuracy. This capability would allow needed supplies to be inserted to a specific area.

**Remote Presence**

Concept no. 900615 is to integrate satellite communications into helmets to provide two-way voice communications. A one-way color camera mounted on the helmet to provide rear-echelon personnel with full visual information is also possible. This concept ties into another SAF need for robust point-to-point communications. The system would be along the lines of an Iridium® system that would place more than dedicated satellites in low-earth orbit (LEO) to provide secure and reliable communications to any individual with the correct equipment and cryptologic material or device.

**Air/Land Assault Craft**

Concept no. 900658 envisions a hybrid of a ground vehicle and a helicopter. The vehicle would be capable of slow in-flight speeds using rotor systems or adjustable thrusters. When in the ground mode, the rotors or thruster would fold and the lightweight vehicles would move on a wheeled drive system.

**Advanced Tactical Transport**

Concept no. 900664 is a VTOL aircraft capable of carrying large payloads to nations that have limited airfields. SAF will need an extremely agile, large cargo transport for both intratheater and intertheater transport. A solution may be the tiltwing, super-short-takeoff and landing, advanced theater transport (Tiltwing

SSTOL ATT). The Tiltwing SSTOL combines extreme short-field capability with autonomous cargo handling to enable deliveries to unprepared landing areas on short notice. The propulsion system may use turboprop or jet engines. Minimum flight speed would be approximately 50 knots, with a field length requirement in excess of 750 feet at high-altitude, hot temperature conditions.

**Camouflage**

Concept no. 900699 would use tiny sensors and electronic devices capable of changing across multiple spectrums to develop camouflage paint or uniforms that blend with the differing terrain. This concept has value for a SAF trying to monitor an area.

**Long-Duration UAVs**

Concept no. 900701 is the development of long-duration UAVs that use solar-powered engines to enhance on-station time. Use of these lighter-than-air vehicles would reduce weight and the power require to move the vehicle around. Lighter-than-air structure would also make the vehicle easier to deploy via heavy-lift aircraft.

**Anti-Sniper Planning**

Concept no. 900705 is a computer-based planning tool that uses a three-dimensional layout of urban areas to predict the most likely location of snipers based upon available fields of fire. The system would aid SAF in determining where surveillance needs to be established and which areas should be secured first.

**Multipurpose Unmanned Aerial Vehicle**

Concept no. 900711 is the development of UAVs with removable line-replaceable units that would permit a quick change of the UAVs payload. Cameras could be replaced with nonlethal or lethal weapons as the situation required.

**Chameleon**

Concept no. 900746 would use optical lenses to generate any color at any angle to make an object look like the environment in which it is operating. Complemented by stealth, chameleon could help aircraft counter radar and optical tracking systems.

**Improved Body Armor**

Concept no. 900753 is improvements in materials technology that could provide a lightweight material for ballistic protection. This material could be molded to fit over the uniforms of SAF members to provide protection not only for the wearer's torso but also for limbs and feet against mines.

**Unmanned Mini-Helicopters**

Concept no. 900763 calls for development of small, remote-controlled helicopters with sensors that could provide reconnaissance of urban areas or, if the vehicle is small enough, of building interiors. The system would require a precise navigation subsystem to permit it to enter confined areas and conduct its mission.

**Personal Identification Friend or Foe**

Concept no. 900906 is a human identification friend or foe (IFF) system to track and identify individuals. UAVs and unmanned reconnaissance systems, equipped with sensors, could provide real time continuous monitoring of SAF personnel in the area.

# Bibliography


AFM 1-1. *Basic Aerospace Doctrine of the United States Air Force.* 2 vols., March 1992.

Alexander, Col John B., PhD. Interview and correspondence with authors, 2–7 April 1996.

________. "Nonlethal and Other Emerging Technologies." Lecture, Air Command and Staff College, Maxwell AFB, Ala., 2 April 1996. Used by permission.

________. "Non-Lethal Weapons Demand Expands as Missions Change." *National DEFENSE* 80, no. 516 (March 1996): 34–35.

________. "Nonlethal Weapons: The Requirements." Unpublished paper, accepted by *Jane's* for publication in upcoming *International Defense Review*, April 1996. Used by permission.

Allard, Kenneth. *Somalia Operations: Lessons Learned.* Institute for National Strategic Studies. Washington, D.C.: National Defense University Press, 1995.

Allotey, Sqn Ldr Sam, et al. "Planning and Execution of Conflict Termination." A research paper presented to the Directorate of Research, Air Command and Staff College, Maxwell AFB, Ala., May 1995.

Arms, Lt Col Anita M. "Strategic Culture: The American Mind." *Air Command and Staff College Theater Air Campaign Studies Coursebook.* Maxwell AFB, Ala.: Air University, 1996.

Barringer, Richard B. *Patterns of Conflict.* Cambridge, Mass: MIT Press, 1972.

Barry, John. "Soon, 'Phasers On Stun'." *Newsweek* 23, no. 6 (7 February 1994): 24–26.

Belton, Beth. "Brown Crash Raises Questions on Trade Missions." *USA Today,* 5 April 1996.

Blaufarb, Douglas S. *The Counterinsurgency Era: US Doctrine and Performance, 1950–Present.* New York: Free Press, 1977.

Brand, Stewart. "Army Green." Originally published in *Whole Earth Review*, no. 76. Edited by Howard Rheingold, on-line, Internet, 14 May 1996, available from gopher://gopher.well.sf.ca.us:70/00/WER/Army/Green.

Builder, Carl H. "Doctrinal Frontiers." *Airpower Journal* 9, no. 4 (Winter 1995): 6–13.

________ and Theodore W. Karasik. "Organizing, Training, and Equipping the Air Force for Crises and Lesser Conflicts." RAND *Project AIR FORCE,* 1995.

Cable, Dr Larry E., PhD. Associate Professor of History, University of North Carolina, Wilmington. *Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War.* New York: New York University Press, 1986.

________. "The Dangers of Dogma." Lecture, Air Command and Staff College, Maxwell AFB, Ala., 28 March 1996. Used by permission.

________. "Getting Found in the Fog: The Nature of Interventionary Peace Operations." Draft. (Compendium of Papers from USAF Special Operations School Symposium), unpublished as of 26 November 1995. Used by permission.

________. "The End State: Why Nations Stop Fighting." Lecture, Air Command and Staff College, Maxwell AFB, Ala., 16 January 1996.

________. Interviews with authors, 31 January and 28 March 1996.

Canby Steven L. "Roles, Missions, and JTFs: Unintended Consequences." *Joint Force Quarterly*, no. 6 (Autumn/Winter 1994–1995): 68–75.

*The Columbia Dictionary of Quotations.* Microsoft ® Bookshelf. New York: Columbia University Press, 1993.

Conference Report: "Professional Military Education and the Emerging Revolution in Military Affairs." Washington, D.C.: National Defense University, 22–23 May 1995.

Dean, Lt Col David J. *Airpower in Small Wars, The British Air Control Experience.* CADRE Paper no. AU-ARI-CP-85-1, Airpower Research Institute. Maxwell AFB, Ala.: Air University Press, April 1985. Originally published in *Air University Review*, July–August 1983 edition.

Dilulio, John J., Jr. "Moral Poverty." *Chicago Tribune*, 15 December 1995.

Donaldson, Maj Howard L. "Constitutional Torts and Military Effectiveness: A Proposed Alternative to the Feres Doctrine." Report Number 83-0565, submitted to the faculty in partial fulfillment of requirements for graduation, Air Command and Staff College, February 1983.

Donovan, David. *Once a Warrior King: Memories of an Officer in Vietnam.* New York: McGraw-Hill, 1985.

Downing, Gen Wayne A. "Joint Special Operations in Peace and War." *Joint Force Quarterly*, no. 8 (Summer 1995): 22–27.

Engelbrecht, Col Joseph A. Comments to draft white paper, March 1996.

Extended Unit Manpower Document, 6th Special Operations Squadron (Foreign Internal Defense), Headquarters Air Force Special Operations Command, 6 March 1996.

Feres Doctrine. *Feres v. United States*, 340 US Code sec. 135 (1950).

"Financial Institutions to Invest Only in Bosnia Reconstruction," *Onasa News Wire*, 1 November 1995, on-line, Internet, available from http://www.axime.com/wm/sarajevo/onasa/9511011002.html.

FM 41-10. *Civil Affairs Operations*, 11 January 1993.

Fuller, Buckminster. "Thinking Out Loud," *An "American Masters" Special.* Public Broadcasting Station, Montgomery, Ala.: 10 April 1996.

Fukuyama, Francis. *The End of History and the Last Man.* New York: Free Press, 1992.

Gourley, Scott R. "The Sniper's Latest Nightmare: Lawrence Livermore Laboratory's LifeGuard System." *International Defense Review* 28, no. 4 (April 1995): 66.

Gray, Colin S. "The Changing Nature of Warfare?" *Naval War College Review* 69, no. 2 (Spring 1996): 7–22.

Hammer, Michael, and James Champy. *Reengineering the Corporation.* New York: Harper Business, 1993.

Hellman, Lawrence C., PhD. "Humanitarian Operations." Lecture, Air Command and Staff College, Maxwell AFB, Ala., 19 January 1996.

Homer-Dixon, Thomas "Tad." "Environmental Change & Violent Conflict." *Scientific American* 268, no. 2 (February 1993): 38–45.

________. "War and Peace." *Maclean's*, 9 January 1995, 19–21.

Huntington, Samuel P. "The Clash of Civilizations." *Foreign Affairs* 72, no. 3 (Summer 1993): 22–49.

________. "New Contingencies, Old Roles." *Joint Force Quarterly*, no. 8 (Autumn 1993): 38–43.

Ikle, Fred Charles. *Every War Must End.* Revised Edition. New York: Columbia University Press, 1991.

Ingersoll, Brig Gen Howard J. "Foot." Received research briefing at Headquarters, Air Force Special Operations Command, Hurlburt Field, Fla., 6 March 1996.

________. Telephone interview. 12 April 1996.

James, Maj Glenn. "Chaos & Campaign Planning." Lecture, Air Command and Staff College, Maxwell AFB, Ala., 8 March 1996.

Joint Warfighting Center. "Joint Task Force Commander's Handbook for Peace Operations." *Air Command and Staff College War Termination Coursebook.* Maxwell AFB, Ala.: Air University Press, January 1996, 64–81.

JP 3-0. *Doctrine for Joint Operations,* 1 February 1995.

Kaplan, Robert D. "The Coming Anarchy." *The Atlantic Monthly* 273, no. 2 (February 1994): 44–76.

Kelley, Lt Gen Jay W. "Brilliant Warrior." ***2025*** white paper (Draft).

Kelly, Kevin. "Shock Wave (Anti-) Warrior." *Wired.* February 1995. On-line, Internet, 14 May 1996, available from http://www.hotwired.com/wired/1.5/features/toffler.html.

Kosko, Bart, PhD. *Fuzzy Thinking, The New Science Of Fuzzy Logic.* New York: Hyperion, 1993.

Lake, Anthony. "Defining Missions, Setting Deadlines." *Defense News* 11, no. 14. On-line, Internet, 14 May 1996, available from http://www.dtic.mil/defenselink/pubs/di96/dill14.html.

Larson, Eric V. "Casualties and Consensus, Domestic Support for US Military Operations." Santa Monica, Calif.: Rand©, 1996.

Libicki, Dr Martin C. "Battlespace Dominance, The Meta-System: Capabilities and Issues." Lecture, Air Command and Staff College, Maxwell AFB, Ala., 25 March 1996.

________. "Project 2025, Institute for National Strategic Studies." Washington, D.C.: National Defense University Press, 1992.

Liddell Hart, B. H. *Strategy.* 1954. New imprint. New York: Meridian, 1991.

Lorenz, Col F. M. "Forging Rules of Engagement: Lessons Learned in Operation United Shield." On-line, Internet, 10 March 1996, available from http://www.cgsc.army.mil/cgsc/milrev/95novdec/lor.htm.

Lucasfilms, Limited. *The Empire Strikes Back.* 20th Century Fox Video, © 1980.

Ludwig, Dr Armin, PhD. "Ecosystemic Violence." ***2025*** lecture, Air War College, Maxwell AFB, Ala., 6 September 1995.

Manchester, William. *American Caesar.* New York: Dell Publishing, 1978.

Manning, Anita. "Monkey Ebola Cases Have Common Source." *USA Today,* 17 April 1996.

________. "Viruses Mutate among Underfed." *USA Today,* 17 April 1996.

McKenzie, Maj Kenneth E., Jr., USMC. "An Ecstasy of Fumbling: Doctrine and Innovation." *Joint Force Quarterly,* no. 10 (Winter 1995–1996): 67–68.

Meilinger, Col Phillip S. "10 Propositions Regarding Air Power." *School of Advanced Airpower Studies.* Air Force History and Museums Program, February 1995.

Montague, Bill, and Christine Dugas. "Peacemakers Slow to Invest in Bosnia." *Pensacola News Journal,* 7 April 1996, 3D. Also entitled "Balkan Region Holds Reward, Heavy Risks." *USA Today,* 5 April 1996.

Morris, Janet, and Chris Morris. "Nonlethal Weapons: Creating New Capabilities for Conflict Management." ©1995. Unpublished paper dated 26 February 1996 in a fax to authors. Used by permission.

________. Numerous telephone interviews with authors, February–March 1996.

________ and Thomas B. Baines. "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." *Airpower Journal,* no. 1 (Spring 1995): 15–29. On-line, Internet, 14 May 1996, available from http://www.cdsar.af.mil/apj/morris.html.

*A National Security Strategy Of Engagement And Enlargement.* Washington, D.C.: Government Printing Office, February 1996.

Nollinger, Mark. "Surrender or We'll Slime You." *Wired,* no. 3.02, February 1995 90–100. On-line, Internet, 14 May 1996, available from http://www.hotwired.com/wired/3.02/departments/electrosphere/nonlethal. html.

O'Connell, Maj Ed. Interview with authors, 25 March 1996.

________. "Nonlethal Concepts: Implications for Air Force Intelligence." first draft, November 1993. Subsequently published in *Airpower Journal* 7, no. 4 (Winter 1994): 26–33.

Perry, William. "Using Military Force When Deterrence Fails." *Defense Issues* 10, no. 80 (6 August 1995). On-line, Internet, available from http://www.dtic.mil/defenselink/pubs/di95/di1080.html.

________. "Managing Danger: Prevent, Deter, Defeat" *Defense Issues* 11, no. 13 (4 March 1996). On-line, Internet, 14 May 1996, available from http://www.dtic.mil/defenselink/pubs/di96/di1113.html.

________. Remarks delivered to the John F. Kennedy School of Government, Harvard University. On-line, Internet, 13 May 1996, available from http://www.dtic.mil/defenselink.

Peters, Thomas J., and Robert H. Waterman, Jr. *In Search of Excellence.* New York: Warner Books, 1982.

Pitts, W. Darrent. "A Guantanamo Diary—Operation Sea Signal." *Joint Force Quarterly,* no. 9 (Autumn 1995): 114–20.

Pomeroy, MSgt Gary. "Perry Lauds Airmen, Airpower." *Air Force News Service.* On-line, Internet, 14 May 1996, available from http://www.dtic.mil/airforcelink/pa/Jan96/an010296/02jan96/960003.html.

Rast, Capt Vicki J., and Maj Bruce R. Sturk. "Coalitions: The Challenge of Effective Command and Control in Support of the Air Campaign." *Air Command and Staff College Theater Air Campaign Studies Coursebook,* 1996.

"ROA National Security Report." *The Officer,* April 1996.

Rodriguez, Lt Col Federico J., PhD. Telephone interviews with authors, 12–28 March 1996.

Seabury, Paul, and Angelo Codevilla. *War Ends & Means.* New York: Basic Books, Inc., 1989.

Schultz, Richard H., Jr. *In the Aftermath of War.* Maxwell AFB, Ala: Air University Press, 1993.

Schwartz, Peter. *The Art of the Long View.* New York: Currency Doubleday, 1991.

Schwarz, Benjamin. "The Diversity Myth: America's Leading Export." *The Atlantic Monthly* 275, no. 5 (May 1995): 57–67.

Shalikashvili, Gen John M. "Force & Diplomacy in the 21st Century." *Institute for Study of Diplomacy Report* 1, no. 1 (November 1994). On-line, Internet, 13 May 1996, available from http://www.georgetown.edu/sfs/programs/isd/files/shali.html.

Sieden, Lloyd Steven. "The Birth of the Geodesic Dome: How Bucky Did It." *The Futurist* 23, no. 6 (November 1989): 14–19.

Snow, Donald M., and Dennis M. Drew. *From Lexington to Desert Storm: War and Politics in the American Experience.* New York: M. E. Sharpe, Inc., 1994.

Story, Lt Col Ann E., and Maj Aryea Gottlieb. "Beyond the Range of Military Operations." *Joint Force Quarterly*, no. 9 (Autumn 1995): 99.

*Strategic Assessment 1996, Instruments of US Power.* Institute for National Strategic Studies, Washington, D.C.: National Defense University Press, 1996.

Szafranski, Col Richard. "A Theory of Information Warfare: Preparing for 2020." *Airpower Journal*, no. 1 (Spring 1995): 56–65. On-line, Internet, 15 May 1996, available from http://www.cdsar.af.mil/apj/szfran.html.

________. "Twelve Propositions Regarding Airpower." *Airpower Journal* 10, no. 1 (Spring 1996): 51–80.

________, and Dr Martin Libicki. ". . . Or Go Down in Flame: An Airpower Manifesto for the 21st Century." Unpublished **2025** white paper. Used by permission.

________. "A SIOP for *Perestroika*?" Air War College Research Report. Maxwell AFB, Ala.: Air University, 1990.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War.* 1993. New imprint. New York: Warner Books Edition, May 1995.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century.* Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

________. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Aircraft and Propulsion Volume, 15 December 1995.

________. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Attack Volume, 15 December 1995.

________. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Directed Energy Volume, 15 December 1995.

________. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Mobility Volume, 15 December 1995.

________. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Sensors Volume, 15 December 1995.

*United States Special Operations Forces Posture Statement 1994.* Honorable H. Allen Holmes, Assistant Secretary of Defense, Special Operations & Low-Intensity Conflict, and Gen Wayne A. Downing, USA, Commander in Chief, US Special Operations Command.

Van Creveld, Martin. *The Transformation of War.* New York: Free Press, 1991.

________. "Transformation of War." **2025** lecture, Maxwell AFB, Ala.: Air War College, 20 September 1995.

Warden, Col John. *Air Campaign: Planning for Combat.* Washington, D. C.: National Defense University Press, 1988.

Widnall, Sheila. "AF Evolving through Contacts with Other Nations." On-line Internet, 14 May 1996, available from http://www.dtic.mil/defenselink.

Wilson, George C. "A Lesson in Peacekeeping." *Air Force Times*, no. 32 (11 March 1996).

Wood, Col Anthony, USMC. "Sea Dragon: Warfighting in the Future." Lecture, Maxwell AFB, Ala.: Air War College, 17 May 1996.

World Health Organization. “Report on the Tuberculosis Epidemic, 1995.” On-line, Internet, 15 May 1996, available from http://www.who.ch/programmes/gtb/tbreport.htm.

“World View: The 1996 Strategic Assessment from the Strategic Studies Institute.” Edited by Earl H. Tilford, Jr. Carlisle Barracks, Pa.: US Army War College, 1996.

*1995 World Refugee Survey.* Washington, D.C.: US Committee For Refugees, Immigration and Refugee Services of America.

Zinni, Lt Gen Anthony C. Commanding General, I Marine Expeditionary Force, Camp Pendleton, Calif. Interview with authors, 29 November 1995.

________. “Commanding in ‘Frontier Missions’.” ***2025*** lecture, Air War College, Maxwell AFB, Ala., 29 November 1995.

***2025*** Concept Papers:

***2025*** Concept, no. 200009. “Pyrotechnic Electromagnetic Pulse.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900153. “Noise Weapons.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900203. “Heavy Lift Aircraft with Mission Pod.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900255. “Inflatable Cities.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900433. “Weekly Food Pill/Shot.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900485. “Guided Airdrop Package.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900615. “Virtual Doctor.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900658. “Urban Assault Helo Vehicle Hybrid.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900664. “Tiltwing Super Short T/O and Landing.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900699. “Chameleon Camouflage.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900701. “Long Duration UAVs (solar powered, long loiter).” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900705. “Anti-Sniper Probability Device.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900711. “Multipurpose UAV.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900746. “Chameleon.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900753. “Full Body Armor.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900763. “Unmanned Mini Helos.” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900906. “Personal Identification Friend or Foe (PIFF).” ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

# Information Operations: A New War-Fighting Capability

Lt Col William Osborne
Maj Scott A. Bethel
Maj Nolen R. Chew
Maj Philip M. Nostrand
Maj YuLin G. Whitehead

## Executive Summary

*The affirming characteristic of Alexander the Great's genius as a general and leader was "the startling rapidity with which he always acted. . . . Time was his constant ally; he capitalized every moment, never pondered on it, and thereby achieved his end before others had settled on their means."*

—J.F.C. Fuller
*The Generalship of Alexander the Great*

In its most basic form, commanders have always performed the functions of observe, orient, decide, and act (OODA Loop) to prosecute military operations.[1] As with Alexander the Great, history shows the military commander who best analyzes, decides, and controls the speed of the engagement prevails in nearly every conflict. To master the OODA Loop, military leaders have pushed technology to obtain more information.[2] Ironically, this situation now leads to the requirement to solve two fundamental challenges if the United States expects to maintain air and space dominance in 2025. First, the proliferation of unintegrated military war-fighting architectures gives the commander potentially conflicting perspectives of the battlespace.[3] Second, the explosion of available information creates an environment of mental overload leading to flawed decision making. Failure to master these challenges critically weakens the military instrument of power. This paper presents a solution to these challenges by confronting commanders as they employ future airpower forces.

Regarding the first challenge, the large number of specialized war-fighting architectures makes information integration supporting overall coordination and control more important and more difficult. Simultaneously, the speed and the range of modern weapons drastically reduces the time commanders have to integrate conflicting information and decide on a course of action.

The second challenge is to harness the information explosion to combat mental overload, thus improving decision making. Recent exercises reveal an alarming number of unread messages because of information overload.[4] As the quantity of data rises, the difficulty of preparing and interpreting it for decision making grows. Traditionally, the military attempted to solve this problem by increasing the number of communications nodes. These past solutions only injected additional inputs and information without improving decision-making capability.

The optimum solution must integrate the functions within the OODA Loop and allow the commander to control the momentum of the cycle. This paper describes how a system, called the Cyber Situation, can do just that, thus optimizing commanders' ability to operate air and space systems. The Cyber Situation enables commanders and decision makers to have in-time access to the

battlespace, characterize the nature of the engagement, determine the calculated probabilities of success from the various authorized lethal or nonlethal options, decide what to do, employ the weapons chosen, and receive in-time feedback on the result of the engagement.

The Cyber Situation system includes five major components. First, all-source information collectors will transmit raw data to the Information Integration Center (IIC), as discussed below. Second, archival databases, linked to the IIC, will be used for historical analyses to fill information gaps if the data is not available for collection. Third, the IIC, an integrated and interconnected constellation of "smart" satellites will analyze, correlate, fuse, and deconflict all relayed data. Fourth, implanted microscopic chips link users to the IIC and create computer-generated mental visualizations.[5] The visualization encompasses the individual and allows the user to place himself into the selected battlespace. Fifth, lethal and nonlethal weapons will be linked to the IIC, allowing authorized users to employ them from the Cyber Situation.

Implied in the Cyber Situation are five key technologies evolving on separate paths that will synergize by 2025 to achieve this goal. They include collection platforms, communications infrastructure, computing power, intelligent software, and human systems and biotechnology. Most of these technologies will evolve through the commercial community, but the military must focus research and development efforts on biological and computational intelligent software and biotechnology breakthroughs to allow mental visualization.

Once realized, these new capabilities will give commanders a new way to prosecute warfare. New technology alone does not revolutionize warfare. Rather, technology's impact on systems evolution, operational tactics, and organizational structure is its true advantage.[6] This fuels necessary and complementary changes in doctrine and organizational structure.

Organizations and doctrine will need to adapt to a streamlined, decentralized environment. The traditional emphasis on command and control will give way to an emphasis on consultation and control. This organizational structure permits the Cyber Situation to operate at maximum efficiency. It also allows commanders' at all levels to operate with a greater degree of latitude and autonomy as part of an integrated joint operation—a truly combined arms.

Airpower in 2025 must make optimum use of information technology to operate inside an opponent's decision cycle. This requires unequivocal dominance of cyberspace. In addition to enabling all military pursuits, information-related activities will transcend all air and space operations.

To be sure, the Cyber Situation proposed in this paper certainly will not eliminate all the command problems facing airpower forces in 2025. However, it may well shed light on the main factors involved and indicate the direction any reform efforts should move. The challenge now is for airpower strategists to develop the war-fighting doctrine to turn the vision of a true battlespace execution capability into reality.

**Notes**

1. Maj David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell AFB, Ala.: Air University Press, February 1995), 16.

2. Examples of technology push to obtain more information range from observation balloons to surveillance and reconnaissance aircraft and satellites.

3. "War-fighting architectures" encompass the entire spectrum of systems (information collection, processing, dissemination; command and control; and offensive and defensive weapons systems) to support military operations.

4. A senior US Department of Defense policymaker lecture given to the 1996 Air Command and Staff College under the promise of nonattribution. The individual stated that during a 1995 Joint Task Force exercise "three thousand of the thirty thousand messages used in the exercise were never opened nor viewed by anyone because of information overload."

5. ***2025*** Concept, No. 900702, "Implanted Tactical Information Display," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

6. Andrew F. Krepinevich, Jr., *War Theory*, vol. 3, *The Military-Technical Revolution: A Preliminary Assessment* (Maxwell AFB, Ala.: Air University Press, September 1995), 163–64.

# Chapter 1

# Introduction

*Victory smiles upon those who anticipate the changes in the character of war, not upon those who wait to adapt themselves after the changes occur.*

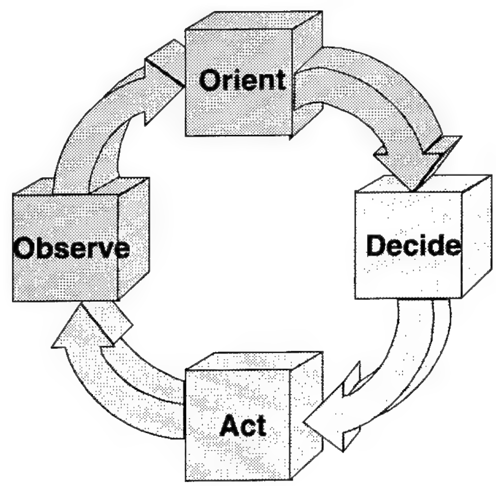
—Giulio Douhet
*The Command of the Air*

*Victory smiles upon those who change the character of war to their advantage, not upon those who merely anticipate the change or wait to adapt themselves after the changes occur.*

—Joseph A. Engelbrecht, Jr.
***2025*** Research Director

## The Challenges

History clearly shows the military commander who best analyzes, decides, and controls the speed of the engagement prevails in nearly every conflict. In the simplest form of conflict, commanders have traditionally performed the functions of observe, orient, decide, and act (OODA Loop) to prosecute military operations (fig. 1-1).[1] To master the OODA Loop, military leaders have pushed technology to obtain more information. This push attempts to achieve the core capability of information dominance that "is the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same."[2] The need for information dominance is vital, because "the emergence of the information and technology age presents new challenges to US strategy even as it offers extraordinary chances to build a better future."[3] In today's world, satellite surveillance and reconnaissance technology provide a unique view of those challenges from the ultimate high ground. Extensive communications links and superior data-processing capabilities allow improved distribution of this information.




**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 1-1. OODA Loop**

Ironically, this situation now leads to two fundamental challenges if the United States expects to continue its dominance of air and space in 2025. First, the proliferation of unintegrated military war-fighting architectures gives commanders potentially conflicting perspectives of the battlespace.[4] Second, the explosion of available information creates an environment of

mental overload leading to flawed decision making. Failure to master these challenges critically weakens the military instrument of power.

The two challenges have resulted in a scenario not unfamiliar to current military operations. Commanders *observe* after waiting for collection assets to assimilate data and analysts to process and interpret the information; *orient* based upon inputs and further interpretations from their staffs that may be conflicting or, worst yet, wrong; *decide* with generally incomplete, imperfect, and possibly biased information; and *act* without first being able to forecast the probability of success of the action or having direct and immediate access to employment tools. Gaps and weaknesses in each step widen and exacerbate as each cycle begins anew.

In 2025 operating near the speed of light will be a common feature of military engagements. Future architectures envision a new array of ground- and space-based sensors, uninhabited combat aerial vehicles (UCAV), and missile defense technology which will take advantage of developing directed energy capabilities. If a kill mechanism operates at the same speed as the flow of information, a defender cannot possess the requisite time to observe the attack, orient himself, decide how to respond, and act on that decision. As a result, the attacker would get inside the defender's OODA Loop, destroying the ability to conduct an active defense.

This paper proposes a solution to these challenges confronting commanders employing future airpower. The optimum solution should integrate the functions within the OODA Loop and allow the commander to control the momentum of the cycle. Further, the solution should enable commanders and decision makers to have in-time access to the battlespace, characterize the nature of the engagement, determine the calculated probabilities of success from the various lethal or nonlethal options authorized, decide what to do, employ the weapons chosen, and receive in-time feedback on the result of the engagement.[5] Simply stated, the solution should go beyond just giving commanders useful information; it should empower them with the ability to leverage information to conduct warfare.

## Assumptions

For planning to achieve information dominance, the following assumptions are plausible for 2025:

1. Information is power. Hence, the high ground of the future will be information dominance.[6]

2. Expect continued explosion in the proliferation of information.[7] The availability of information is overwhelming, and the driving issue that will contribute to success is being able to sift the "gold from the dross."[8] Accordingly, collection assets, regardless of where they are based, will be sufficiently available in 2025.

3. The site, size, and scope of future conflicts are unknown. The United States military must be prepared to fight or to conduct mobility or special operations anywhere in the world on short notice.[9]

4. The military will have to fight at long distances from the United States. In particular, some operations may be staged directly from the continental United States. These operations may endure for weeks or months in weather conditions executed both during the day and night.[10]

5. Adversary capabilities steadily will improve and will be difficult to forecast.[11] The United States must assume we will fight smart enemies who have analyzed all aspects of our military doctrine, capabilities, and operations. Further, they will develop weapon systems to attack their perceived vulnerabilities of United States military forces.

6. Military personnel strength will continue to decrease, thus placing further importance on optimizing individual performance.[12]

7. Today's principles of war will still be applicable in 2025.[13] They include the need to gain the offensive, achieve unity of command, maintain security, exploit surprise, use mass and maneuver while practicing simplicity, and employ economy of force.

## The Rest of the Story

The remainder of this paper discusses the proposed solution and its implications. Chapter 2 explains the required capability by outlining the need for OODA Loop integration and momentum control. Chapters 3 and 4 take the reader through the technology evolution that synergizes in the solution called Cyber Situation. Chapter 5 discusses vulnerabilities and countermeasures. Chapter 6 outlines how the Cyber Situation functions and its implications on doctrine, tactics, organization, and force structures. Finally, chapter 7 recommends areas requiring additional research, and chapter 8 offers a conclusion to this paper.

Overall, this paper focuses on the conceptual fusion of information operations. Other ***2025*** papers deal specifically with various aspects of information operations.[14] Furthermore, other papers focus on technologies this paper assumes will be available in 2025, including space lift, uninhibited aerial vehicles (UAV), and other lethal weapons.[15] This paper serves as the integrator of future information operations technology—a concept that enables military commanders to observe the battlespace, analyze events, and direct forces from within a single entity.

#### Notes

1. Maj David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis* (Maxwell AFB, Ala.: Air University Press, February 1995), 16.

2. Dr Sheila E. Widnall and Gen Ronald R. Fogelman, *Air Force Executive Guidance* (Washington, D. C.: December 1995), 2, 17. This document outlines five Air Force areas of core competency—air superiority, space superiority, global mobility, precision employment, and information dominance.

3. William J. Clinton, *A National Security Strategy of Engagement and Enlargement* (Washington, D.C.: White House, February 1996), 1.

4. "War-fighting architectures" encompass the entire spectrum of systems (information collection, processing, dissemination; command and control; and offensive and defensive weapons systems) to support military operations.

5. The use of "in-time" as opposed to real-time or near-real time puts the focus on both timeliness and requirement for information. In-time access means getting information to users *in time* to perform a mission or task.

6. Widnall and Fogelman, 16.

7. Martin C. Libicki, *The Mesh and the Net: Speculation on Armed Conflict in a Time of Free Silicon* (Washington, D. C.: National Defense University Press, 1994), 2–3.

8. Francis Fukuyama, RAND, Electronic Mail, subject: Dross and Gold, 27 December 1995. Used by permission of author. This electronic mail stresses the importance of "sorting the gold from the dross" because of "data deluge" and the problem of "facing too much wrong information, a phenomenon often exacerbated by new information systems."

9. Air Force Scientific Advisory Board, "New World Vistas, Air and Space Power for the 21st Century" (unpublished draft, 15 December 1995), 5.

10. Ibid.

11. Ibid.

12. Ibid.

13. AFM 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 1, March 1992, 16.

14. Other ***2025*** Study research papers dealing with aspects of information operations include: Maj Cindy Norman et al., "Man In the Chair" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); Maj Mike Tiernan et al., "In-Time Information Integration System" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); and Maj Barbara Jefts et al., "Virtual Integrated Planning and Execution Resources System: The High Ground of 2025" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996).

15. Other ***2025*** Study research papers dealing with spacelift, UAVs and lethal weapons include: Lt Col Bruce Carmichael et al., "StrikeStar 2025" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); Lt Col Henry Baird et al., "Spacelift" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996); and Maj Philip Simonsen et al., "On-Orbit Support" (Unpublished paper, Air University, Maxwell AFB, Ala., April 1996).

## Chapter 2

# Required Capability

*Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the mind of humans. That's where the battles are won.*

—Col John Boyd

### Information Dominance

As a new millennium approaches, information dominance should become a "blue print" for continued success as a superpower and contribute to peace particularly by adding new dimensions to deterrence.[1] Currently, information operations focuses too narrowly on the acquisition, transmission, and storage of information. Today's *Cornerstones of Information Warfare* defines military information functions (operations) as surveillance, reconnaissance, command and control, intelligence, communications, combat identification, precision navigation, and weather.[2] In 2025 the definition will likely include tools that allow military leaders to integrate seamlessly the functions of the OODA Loop and the ability to control momentum.

### Speed and Accuracy of OODA Loops

Every individual operates an OODA Loop that is unique in speed and accuracy (fig. 1-1). Speed is based on the individual's mental capacity and capability to deal with information and changing environments. John Boyd asserts that one can paralyze an enemy by operating inside his OODA Loop, meaning that the individual is operating a faster cycle speed than the enemy's.[3] Accuracy is determined during the orient part of the cycle by what information is filtered and how it is organized. Boyd considers the orientation as the most important part of the cycle because "it shapes the way we interact with the environment—hence orientation shapes the way we observe, the way we decide, the way we act."[4]

### Dross versus Gold

Increasingly, the OODA cycle time is affected by a growing deluge of information, with much of it insignificant or not applicable to the task at hand.[5] The difficulty lies in filtering out exactly the nuggets of information that are useful. Unfortunately, during combat operations, most commanders possess limited time to perform specific tasks and issue orders. Further, as increased volumes of information are input into the OODA Loop or as the rate of input increases, natural defense mechanisms tend to try to protect people.[6] A key mechanism is a "bounded rationality"[7] that allows individuals to screen out inputs prior to being overloaded or inundated so they can continue to focus on a particular task. One danger lies in the commanders screening out "golden nuggets" because they are focused elsewhere. A second danger lies in failing to recognize when new data should dictate a refocus or reorientation.

### OODA Loop "Integration"

Technology, however, can integrate functions within the OODA Loop and speed up the cycle. It does this by creating decision support tools to alleviate the precarious situation that exists when crucial nuggets of information are omitted from the individual's OODA Loop. The tools,

designed especially for commanders, would aid in managing military information to fit how commanders actually assess situations and issue orders.[8] The decision support tools would assist commanders to deal with inputs from different, sometimes contradictory or incremental, sources. Unfortunately, the integration tools do not currently exist. This paper proposes the development of this capability in subsequent chapters.

## "Momentum Control"

Thus far, we have assumed that technology will assist the commander by increasing the speed and improving the accuracy of his OODA Loop. However, it is also possible successful military operations will require a "loosening" of the loop.[9] Specifically, technology should also allow the commander to "control momentum" of the OODA Loop. In other words, the commander must be able to control the cycle speed to allow the "modulation of both time and space" so the "impulse of strategic power is imparted at the proper moment to the objective at a critical position."[10] The final stage of employing or impulsing the strategic power must be "kept short so as to minimize the enemy's ability to avoid the onslaught or effect countermeasures."[11]

"Momentum control" is an unorthodox concept because the information age compels users to believe that faster and shorter OODA Loop cycles are the goal. However, there may be opportunities where slowing the cycle benefits the commander's operations and induces friction in the enemy's cycle. Momentum control includes the ability to operate within the desired time cycles, both by controlling friendly movement and by affecting an enemy's movement.[12] For example, a special operations soldier camouflaged to match the terrain will move relatively fast toward an enemy camp. Yet, once he is within viewing distance of the enemy, his movement slows to a minuscule rate to prevent enemy detection. The soldier has slowed his OODA Loop cycle by controlling momentum in both time and space. Another example is the strategic football coach whose team has a lead late in the fourth quarter and who employs the running game when his team is on offense. Like the soldier, the savvy coach wants to control the momentum of the battle, to slow the OODA Cycle by using time (the clock continues to tick between running plays) and space (achieving enough yards every three or four plays to get a first down) to defeat the opposition. The opposition, in turn, tries to regain momentum control by calling time outs to break the cycle of the team on the offense.

## OODA Loop Tasks and Attributes

Tables 1 to 4 list tasks and attributes of each OODA Loop function to demonstrate what should be integrated to enable commanders to control momentum. The objective is to use the tasks and attributes as measures for how effectively both individual functions and the integrated OODA Loop operates when 2025 technology is applied. Further, the tasks and how

**Table 1**

**Observe Tasks and Attributes**

| TASKS | ATTRIBUTES |
|---|---|
| See the battlespace | • Fused, integrated, deconflicted view of the desired battlespace<br>• Sum of all possible information sources<br>• System identification of information gaps and subsequent collection of missing information |
| Maintain mobile battlespace view | • Able to pull updated view anytime, anywhere<br>• Easily deployable and transportable with user |
| Universal access to battlespace view | • Able to tailor picture for relevant AOR, missions, and tasks<br>• Many able to see the same battlespace picture |

**Table 2**

**Orient Tasks and Attributes**

| TASKS | ATTRIBUTES |
|---|---|
| Tailor view of the battlespace | • In-time view of the battlespace<br>• Able to define dimensions and locations of battlespace |
| Comprehend the battlespace view | • Eliminate biased inputs from one person to another<br>• Eliminate need for mental picture based on another's biases<br>• Able to query for further information; receive in-time answers |

**Table 3**

**Decide Tasks and Attributes**

| TASKS | ATTRIBUTES |
|---|---|
| Decide what is important and what may require action | • Decision support tool in transmitter and receiver to filter, sort, and prioritize<br>• Prompts user of significant events for monitoring and action |
| Determine action required to rectify undesirable situation | • Model effectiveness of potential actions and inactions with in-time feedback<br>• Optimize application of precision force<br>• Ensure least risk to friendly forces |

**Table 4**

**Act Tasks and Attributes**

| TASKS | ATTRIBUTES |
|---|---|
| Immediate access to assets to rectify undesirable situation | • Ready lethal capabilities for employment<br>• Ready nonlethal capabilities for employment<br>• One shot, one kill capability |
| Feedback on actions and inactions taken | • See in-time mission results<br>• System recommends additional action or inaction |

attributes serve as measures of merit to determine which technologies discussed in the next chapter meet the requirements to achieve OODA Loop integration. Ultimately, the evolving technologies that rate best seem most appropriate to pursue for system development.

**Notes**

1. The concept of a "blue print" has guided US Air Force modernization in the past. Gen Ronald R. Fogleman, chief of staff, US Air Force, stated in a lecture delivered to the ***2025*** project participants at Air University, Maxwell AFB, Alabama, 13 February 1996: "Force Modernization is the blue print for [today's tenets of] Global Reach and Global Power. Our strategic vision remains containment through deterrence." To actualize this vision, the Air Force reorganized into Air Mobility Command (Global Reach) and Air Combat Command (Global Power). Further, the 1990s witnessed the Air Force leadership promote the C-17 as the key short-term solution for Global Reach, and the F-22 for Global Power.

2. Dr Sheila E. Widnall and Gen Ronald R. Fogelman, *Cornerstones of Information Warfare* (Washington, D. C.: 1995), 3.

3. Fadok, 2.

4. 1st Lt Gary A. Vincent, *Operational Structures*, vol. 5, *In the Loop: Superiority in Command and Control* (Maxwell AFB, Ala.: Air University Press, November 1995), 291.

5. Fukuyama.

6. Jeffrey McKitrick et al., *The Revolution in Military Affairs*, Air War College Studies in National Security: Battlefield of the Future, no. 3 (Maxwell AFB, Ala.: Air University Press, September 1995), 65–97.

7. Herbert A. Simon, *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization* (New York: The Free Press, 1976), 38–41.

8. Lt Col Michael L. McGinnis and Maj George F. Stone III, "Decision Support Technology," *Military Review* 74, no. 11 (November 1994): 68.

9. Col Richard Szafranski and Col Joseph A. Engelbrecht, Jr., "The Structure of the Revolution:

Demystifying the RMA" (Unpublished paper, March 1996), 6–7. The authors used the term *momentum control* to explain time. However, "time is more than speed. It is the attribute of controlled timing or modulating momentum." See also endnote 10, this chapter.

10. Ralph D. Sawyer, *The Seven Military Classics of Ancient China* (Boulder, Colo.: Westview Press, 1993), 442. The concept and description of "momentum control" was derived from the Chinese term, *chieh*, translated as "constraints," which is commonly used to indicate constraints or measures imposed on troops. The term lacks a satisfactory English translation because it encompasses the concepts of "control," "timing," and "measure." See also endnote 9, this chapter.

11. Ibid.

12. Szafranski and Engelbrecht, 6–7.

## Chapter 3

# Technology Investigation

*What the warrior needs: a fused real-time, true representation of the warrior's battlespace and the ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute his mission in that battlespace.*

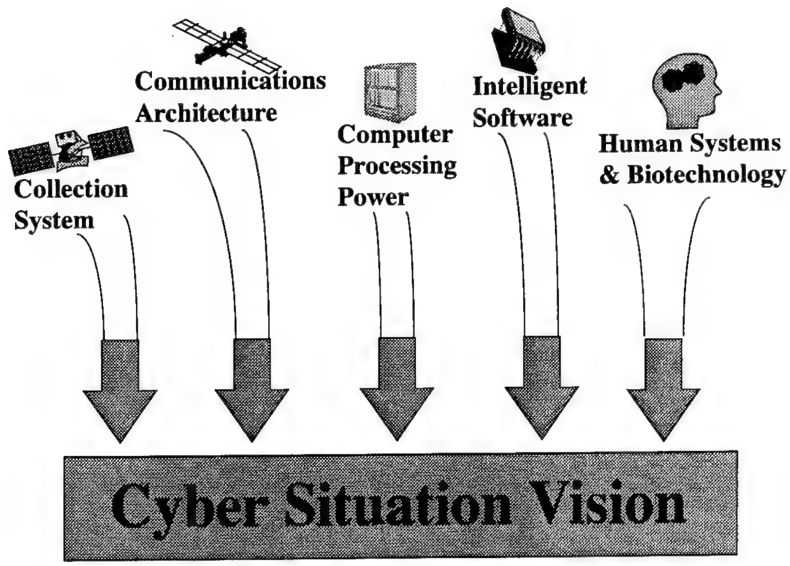
—Adm Richard C. Macke
*C4I for the Warrior*

In 1992 Adm Richard C. Macke understood what war fighters since Alexander the Great wanted. Information operations is a legitimate and increasingly important military mission that seeks to satisfy Admiral Macke's requirement.[1] Perfecting this capability should allow US military leaders to achieve information dominance and control the momentum of military operations. This vision does not merely provide information, but also empowers users with the ability to leverage information to conduct warfare. This paper refers to this vision as the Cyber Situation. The Cyber Situation is necessary for the US military to maintain its competitive edge against future adversaries.

Technology will provide the means to achieve a complete battlespace picture and the ability to affect it instantly with the Cyber Situation concept. This chapter lays the technological foundation which could achieve this capability. Five broad technology areas should contribute to reaching this goal. Some solutions appear to be evolutionary; some will likely be wildcards—scientifically plausible achievements that will require a technology leap.[2] While this chapter describes the technologies, the next chapter applies these technologies and assesses their contribution to a single system to achieve the Cyber Situation vision.

The Cyber Situation will require five technology areas to evolve and synergize by 2025 to achieve OODA Loop integration. First, collection platforms should provide a detailed global awareness, giving decision makers a complete situational picture.[3] This parallels the observe function of OODA. Second, communications systems should advance to allow in-time access to virtually any available database. Communications will permit information flow around the loop. Third, computer-processing power and, fourth, intelligent software will provide the ability to integrate and correlate disparate types and sources of information and aid in decision making, contributing to the orient and decide functions. Fifth, human systems and biotechnology advancements will make the man-computer interface seamless. The end result should be an improved ability to access and direct weapons.[4] Figure 3-1 illustrates these essential technologies.

The following sections address each of these broad technology areas. Within each section, the discussion first relates the particular technology to the required capability in terms of the OODA tasks and attributes (tables 1 through 4). Next, it assesses the current state of the technology and notes which are on evolutionary or revolutionary tracks. It then evaluates various research and development (R&D) trends, focusing on the time and cost needed to achieve the desired technological capability. Most of the development will be in the commercial arena. Special recognition will be made for those developments that require a military investment.




**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 3-1. Battlespace Vision: Key Components**

## Collection Platforms

Collection is the process of capturing information from all sources to present an in-time "picture" of the battlespace. In this case, picture refers to more than an image. It is all surveillance and reconnaissance data, including imagery, signals intelligence, weather data, aircraft radar navigation equipment transmissions, cellular telephones and communications devices intercepts, and data in-transit between computers. The list is virtually endless. All information is potentially useful to the Cyber Situation. However, it is not this paper's purpose to exhaustively review all collection technologies. Rather, it will focus on the platforms from which the data and intelligence is received.

Presently, overhead and air-breathing assets collect information. Overhead assets refers to satellite-based systems. They include surveillance, reconnaissance, and target acquisition systems as well as environmental monitoring assets.[5] While many are classified programs, civil and commercial agencies are increasingly able to collect more timely and detailed data. This is particularly true for such environmental monitoring satellites as the French SPOT satellite which can provide multispectral imagery with 10-meter resolution.[6] Air-breathing assets are aircraft, manned or unmanned.

By 2025 collection platforms will exploit the complete electro-optical frequency spectra. Some systems will be deployed for long durations. These systems will observe such standing requirements as military communications traffic, logistics, and computer interfaces. Some of this capability currently exists. However, the military still lacks sufficiently broad coverage.[7] Other systems may be used on a contingency basis. These systems will use two emerging technologies: miniaturized satellites and uninhibited reconnaissance aerial vehicles (URAV).

### Miniature Satellites

The most compelling satellite technologies advances include miniaturization and decreased launch expense.[8] These two complementary advances are important to

the system effectiveness of the Cyber Situation. Increased miniaturization of individual satellites allows for less costly construction per unit and easier deployment while at the same time making them harder to detect and track. Miniature satellite constellations have great applicability in terms of flexibility and deployability.

Miniature satellites could fill coverage gaps to supplement long-duration systems. The miniature satellite constellations would carry payloads optimized for specific contingencies. The payloads may focus on specific static, mobile, or moving targets. This option offers a compelling, inexpensive, and rapidly deployable solution to "customize" collection efforts to meet the contingency needs.[9] The satellites may be constructed en masse and be on hot alert.

While decreased cost for space access is forecasted, miniature satellites are unlikely to garner significant commercial investment. This is not to say miniature components will not be commercially available. Commercial technology initiatives will shrink everything from the solar panels and batteries to the sensors. However, the military must press forward with the R&D to package miniature satellites and make them available for immediate use.

#### Uninhabited Reconnaissance Aerospace Vehicles

The other emerging technology area for collection platforms is URAV. These systems would provide the data not accessible to either the long-duration assets or the miniature satellite constellations. URAV would reduce the risk inherent in manned collection platforms and allow the flexibility to maneuver rapidly to specific locations, which may be obscured from space-based sensors.[10]

The Department of Defense has operated URAV since the Vietnam conflict. Their usefulness will push development of less costly, more reliable, and more flexible systems.[11] One area of flexibility will include more varied sensors that collect all-source information. This area will predominately require military R&D.

The combination of deployed long-duration satellites, small satellites, and URAV could enable the military to achieve broad coverage of an area of interest virtually all of the time, thus providing the user the most updated Cyber Situation possible.

### Communication Infrastructure

To achieve information dominance requires high-capacity, secure, accurate, reliable, robust, and easy-to-use communications. Indeed, data and information movement is the track upon which the decision cycle runs. A highly mobile war fighter must be able to maintain an in-time "picture" of the battlespace, formed by vast amounts of information from multiple sources. The user must also be able to communicate with others who are observing the same battlespace picture. Of particular importance is the ability to access and direct weapons at a moment's notice.

Communications must work anywhere and everywhere. Current limitations include narrow bandwidths and insufficient ground-based and satellite infrastructure. In 2025 these limitations will likely be resolved as bandwidth and communications capacities continue to expand.[12]

Although bandwidth is a limiting factor, it has grown dramatically in the last 10 years. The key breakthrough was fiber-optic cabling, which geometrically increased available information flow. Economics drove the development of fiber-optic capability. The marketplace demanded increased throughput, and the private sector responded with a quantum leap over twisted pair (copper wire) technology. Demand will continue to push increased access throughout the country and around the world.[13] Fiber-optic cable will likely be the predominant communication carrier for the foreseeable future, although wireless and satellite communications connectivity also will be required.[14]

Satellite communications are tremendously important because of the need to move large amounts of the information from collection platforms. Current capabilities are inadequate to provide full connectivity and functionality to provide coverage for any given desired place and time. Here, too, technology advances will greatly enhance and improve the ability to move vast amounts of data quickly.

As noted in the previous section, the most compelling satellite technologies advances include miniaturization and decreased launch expense. A significant amount of work has already has been done on the miniaturization of relay and broadcast satellites. To date, experiments have centered on deploying these small satellites over a location where the telecommunications infrastructure is lacking.[15]

On the ground, direct broadcast satellite (DBS) technology use will release commanders and decision makers from the bonds of landlines. It is a fully man-portable satellite receive and transmit ground station. DBS is commercially available at reasonable cost. DBS groundstations will be able to accommodate large bandwidth and be fully deployable.[16] This is a distinct advantage in terms of flexibility for decision makers at all levels. DBS technology allows on-scene commanders to forward in-time inputs through the system and up the chain of command. Future DBS technology will continue to advance and miniaturize, producing greater capabilities in smaller packages. One challenge is to be able to provide portable power that is not a weight and size burden. Nevertheless, the commercial industry will produce miniaturized, low-power communication devices. As this type of technology improves, DBS might allow human links to satellites. The human body could potentially become a part of the system. "With a little digital help, people's ears could work just as well as 'rabbit ears.'"[17]

Mission accomplishment requires the communications architecture to accurately transmit complete media spectra. More important is the Cyber Situation's need for secure communications. This is a broad category requiring a more detailed discussion.

**Security**

Since security affects all elements of the OODA Loop, it is best addressed under the communications section. Data must be secured in three different areas: storage, transmission, and dissemination.

Because of the tremendous storage capacity required, archival databases likely will be secured much as they are now, in a vaulted building on shielded media (magnetic, or some evolutionary storage media not yet developed). Storage is discussed in the computer power section below.

The compromise potential is much higher during data transmission. It occurs during information collection and routing by way of communications infrastructures. Resident safeguards must protect transmissions from interruption and intercept. Experts expect that this should be easily attained by way of commercially available encryption packages that are nearly unbreakable.[18]

The final security concern involves the process to retrieve, display, and use data. Dissemination security exists to ensure that only those with the appropriate access and need to know may use the most sensitive databases. Some promising technologies are already used in this area. Among the most viable are retinal scanners and fingerprint validation technologies developed by the private sector.[19]

Technology could plausibly lead to the use of deoxyribonucleic acid (DNA) samples to validate individual access requirements. The validation system will include each user's DNA imprints, which must be checked before the system allows access. Today, this technology is in its infancy, but, will continue to evolve and likely become the foolproof way to validate user authenticity for access and employment.

The second type of dissemination security involves technology known as multilevel

security (MLS) network management.[20] Upon entering an information system, the system grants access based on the user's authorization. Ideally, MLS allows users with various classification levels to share the same communication architecture and even the same sensors. The difference lies in what each user is able to access in each situation. Since the mid-1980s, the civilian and military communities have conducted R&D in MLS technology. However, the state of technology does not currently allow ideal MLS use. It is reasonable to expect a perfected system by 2025.[21]

### Communications Wrap-Up

In large measures, the commercial and military communities already have established necessary communications infrastructure with the National Information Infrastructure (NII) and the Military Information Infrastructure (MII). Both NII and MII are structured to move information in the most expeditious manner, taking advantage of the best of commercial and military communications links. "The MII must able to adapt to unforeseen circumstances, whether induced by the military or by the commercial world. . . . It becomes more important to learn to use existing and emerging capabilities in the domain of military applications than it is to develop the capabilities themselves."[22] Thus, the groundwork is already laid for expansion and evolution.

Nevertheless, to fully achieve the 2025 Cyber Situation, a global infrastructure must provide the user a desired view anywhere on earth. Therefore, the 2025 information infrastructure must incorporate both NII and MII—leading to a Global Information Infrastructure (GII).[23]

Effective communications architectures must be robust to accommodate the considerable bandwidth requirements and to harness the full capability of military and civilian communications advances. This leads to the next topic, computer power.

## Computer Power

If communications is the track on which the OODA Loop runs, powerful computers is the engines pulling the train. Computers will play a key role in any decision support system to integrate the collected data and present it for orientation and decision making.

Powerful computers with massive storage capacity will be essential in the Cyber Situation. Fortunately, the rapid increases in processing speed and storage, combined with decreased size and energy consumption, will likely continue unabated.[24]

While silicon circuit technology remains viable for the near future, eventually the number of circuits that can be etched will reach a limit.[25] However, researchers are pursuing alternative technologies that should result in even more amazing improvements. They include such exotic concepts as quantum dots and nanomechanical gates.[26]

Biological computing is another promising field which might yield a potential thousandfold computational improvement for one ten-millionth the energy.[27] The concept includes using genetic material from insects to self-assemble into computing elements. House flies and grasshoppers have pattern-recognition abilities which could be applied directly for military and commercial purposes, including cryptography and navigational computation. Initial payoffs to molecular biology computing research may occur in five to 10 years, especially for sensor applications.[28]

Increased speed requires improved data storage media. Again, research shows promise. Holographic memory may allow storage of 64 billion bits on a crystal the size of a compact disk. Activated by a small laser, a single "disk" could contain over 600 hours of music or 30 million pages of double-spaced, typewritten text.[29] Since the data is contained in the laser, it makes it easy to transmit in optical cable as well.[30]

Clearly, by 2025 nearly infinite computations with unlimited storage will be available on tiny machines. It should come

with negligible military investment although the *New World Vistas* (NWV) Information Technology Panel warns that defense should continue to fund basic research to keep the "pump primed," else risk less innovation as private research focuses on highly directed problems.[31] However, the challenges of storage capacity and capability are not the only areas where researchers are trying to stretch the limits. More importantly are increasing the cognitive abilities of the software running on these powerful machines.

## Intelligent Software

The most important technology area is the continued advancement of intelligent software. The previous technologies explained how vast quantities of information will be readily available to the war fighter. Without some assistance in managing the load, the commander will suffer from information overload.

Intelligent software is broadly defined as the component programs and algorithms executing on various computer systems. While primarily related to the human's use of the program, it also may operate independently of the user. For example, the collection systems will be able to recognize and identify features, identify information gaps and task a sensor to "fill in the gap," fuse multiple data sources to present an integrated picture, and prompt a user of significant events, all without human assistance. Other software agents will respond to human taskings or augment humans in decision processes.[32] Attributes include the ability to organize and interpret information, simulate and model potential actions, weigh alternatives, and recommend courses of action.

The following paradigm applies for all intelligent systems (biological or computational). This paradigm helps identify and measure the broad intelligent software tools needed for the Cyber Situation.

All intelligent systems continuously engage in five activities:

- They *perceive* the world.
- They *interpret* their perceptions in light of their knowledge of the world.
- They *make plans* based on their current model of the world.
- They *act* within the world in order to achieve their goals.
- They *communicate* with other agents to share perceptions and collaborate on execution (emphasis added).[33]

Note the elements of Boyd's OODA Loop in this concept. Many of today's experts envision technological advances will occur in all activities to assist the decision maker. Indeed, the Cyber Situation assumes double-leap improvements in the ability to observe, act, and communicate. The concept focuses on the interpretation and planning activities and how to make the best use of information to plan and execute a military operation.

Intelligent software can be broken down into four broad core technologies.[34]

### Image Understanding

Image understanding (IU) seeks to develop mechanisms to create a "description" of the world from sensor images, suitable for particular purposes. The challenge is identification "despite object occlusion, shadows, reflections, and other disturbances."[35] Applying contextual information may be one mechanism to improve the IU process.

IU is a key technology because the Cyber Situation must generate and communicate situational awareness to the user. Within five years, the DOD's Advanced Research Project Agency (ARPA) expects "to carry out applications-directed research on machine vision, provide a suitable IU software environment, and further develop IU capabilities for specific applications." The long-term goal is to "develop computational theories and techniques for use in artificial vision systems whose performance matches or exceeds that of humans, exploiting sensing throughout the breadth of the electromagnetic spectrum, in all environments."[36] Commercial applications include industrial part recognition, visual inspection

systems, and indoor robot navigation. However, because of the predominance of military applications, this is a technology requiring DOD investment.

**Intelligent Integration of Information**

Intelligent integration of information (I3) is the technology to "intelligently process, compile, and abstract useful knowledge from multiple data sources with different interfaces, query languages, data structures, terminology, and semantics."[37] This ability has applications throughout the Cyber Situation. I3 is needed to provide the fused, deconflicted view of the battlespace.

Many valuable applications have been developed. An example is the Air Campaign Planning Tool where planners can now locate high-priority targets in a fraction of the time previously required.[38] However, much work remains to achieve large-scale applications which abstract data from the entire GII. Although commercial applications will push the technology (resulting, for example, in personal assistant agents sorting increasing amounts of daily electronic mail),[39] the military must invest to obtain the ability to index and then retrieve images based on military semantics.[40]

**Planning and Decision Aids**

Planning and decision aids (PDA) tools develop representation and reasoning techniques to generate and analyze plans and schedules. These tools are necessary to help the user (or users) make correct and timely decisions, thus deconflicting information overload. The tools will "reduce problem solving time by orders of magnitude while at the same time increasing the number of options considered by orders of magnitude."[41]

The concept of PDAs is well understood, as it is simply an implementation of such decision theories as linear programming and quantitative analysis. What is new is the ability to employ these techniques on a high-speed computer. Many techniques already exist, both in private and military use. One example is the Dynamic Analysis and Replanning Tool which was used in Desert Storm.[42] Commercial applications, both executive and group support systems, also are being adapted for military use. The military must focus on ensuring more than one user can use them simultaneously and that the tools capture the planning rationale.[43]

**Human Computer Interaction**

Human computer interaction (HCI) will "develop techniques and environments to provide informative, intuitive, and taskable access and control over complex software."[44] This environment is another key area for the Cyber Situation—being able to "interact in a natural fashion with speech, gesture, and other advanced interaction techniques." Eventually, it should include brain activated control. A goal is for many users to interact over computer networks.

Initially, human language system advances will be where the most significant work is done. However, the NWV Information Technology Panel suggests handwriting recognition will become prevalent as well as speech recognition capabilities within 10 years. While the currently dominant keyboard-display-mouse configuration will remain, newer generations of users will become more comfortable with more natural interfaces. By 2025 technology will have matured such that handheld, portable "personal assistants" will be available. Additionally, virtual and augmented reality systems and telepresence models also will be in use. Telepresence models allow a human access to otherwise inaccessible locations. Applications include microsurgery, space system repair, and microelectronic machine assembly.[45]

The NWV Human Systems and Biotechnology Panel describes neuroscience as a promising research area. As science improves our understanding of the brain and how it functions, it makes it possible to direct equipment to respond to our thoughts,

without any verbal or written command. Already, preliminary research using an 128-sensor array electroencephalograph (EEG) pressed against a subject's skull can "influence information content and display designs on a computer screen."[46] This concept is discussed further in the next section. Commercial and medical organizations will take the lead in developing this technology. Neuroscience developments will continue.

## Human Systems and Biotechnology

The human-computer systems integration is a vital lead-in to the final technology area. Human systems and biotechnology offers the potential to create a seamless flow of information between human and computer. By exploiting the human cognitive process, it can tailor information to present precisely what is needed.

This section is divided into two parts. The first is understanding information flowing to and from the brain. The second is how to present that data using visual-imaging techniques. Mastering these technologies will allow users to select information for direct input into their brains. However, regardless of how advanced a decision system becomes, a human will be in the loop. The best technology can only help, but in the end, the person, not the machine, ultimately makes the decision.

### Charting the Brain

Thirty years ago little was known about the brain. Great advances have been made in the last 10 years, and much has been learned about information flow out of the brain and the way it interacts with the neural network.[47] Understanding how information enters the brain and how it is processed will form the foundation for the ultimate in human-computer interface. "Success in transducing and translating brain waves allows people to interface with specific systems, perhaps sensed through transducers in a headband or another such brain-machine connection."[48]

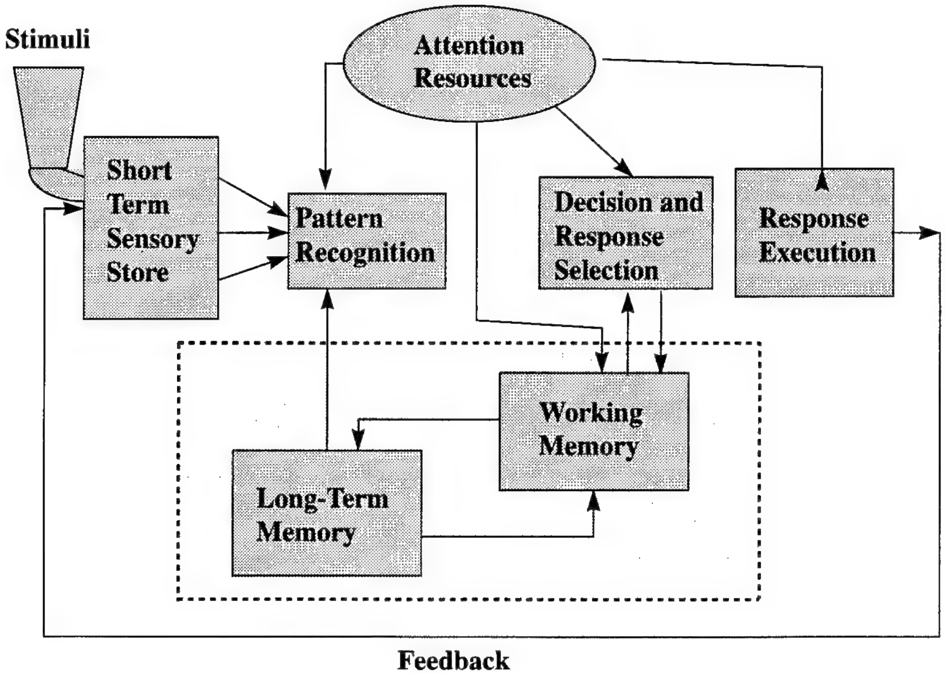
Two research areas are critical to the human computer interface. The first of these is charting and understanding information flow out of the brain. The second, and more applicable, is information flow into the brain. Understanding of human systems such will enable more rapid processing of data and more efficient use of the provided information.

Charting information out of the brain is a complex effort. However, much work has been done in this area.[49] Mechanical methods have been fielded to emulate, and in some cases replicate, these complex processes.[50] Intelligent materials, including fiber-optics and piezioelectric materials, are two techniques under development to try to replace damaged or destroyed neuron-actuation sensor networks in humans.[51]

In principle, data flowing out of the brain is in the form of electronic impulses which actuate the neurostructure within humans.[52] Recent research has charted the source of some basic impulses within the brain, identified precisely what neuron network is actuated by electric impulses, and determined what action is completed by the network.[53]

Charting information flow *into* the brain and how the brain processes it once inside is even more difficult. This effort requires understanding how the brain formats the data to make decisions. Each human's information process is unique, based on such factors as experiences, learning, intelligence, and personal biases.[54] Science is attempting to understand the commonalities between humans.[55] Some work has been done to chart the essentials of human information processing (fig. 3-2).[56]

Computers can play a significant role in nearly every area of human-information processing.[57] Their potential lies in organizing information to assist human decision making. They can produce more options than a human brain can recall.[58] In fact,




**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 3-2. Human Information Processing Flow**

computers have become the preferred medium for information storage and recall.[59]

However, a gap still exists in the information flow between humans and computers. Information is processed by a human looking at a screen, reading the data, and translating it into something useful through internal thought. "We talk longingly about human-computer interactions and conversational systems, and yet we are fully prepared to leave one participant in this dialogue totally in the dark. It is time to make computers see and hear."[60] Users should "converse" with computers. Intelligent systems outlined above provide only part of the answer to improve human-computer interaction. The missing piece is a better way to format and transmit information from the digital computer processor in the computer chip to the analog processor in the human brain.

Instead of formatting a cathode ray tube (CRT) to more easily access and display data, a computer can be designed and programmed to bypass the CRT and format information which can be immediately processed by the brain. The logical extension would be to place the human computer interface directly in the brain. Some significant progress already has been made in this area by the Stanford University research center and their development of a nerve chip.

> It is an electronic interface for individual nerve cells to communicate with a computer. This human-machine linkage will . . . enhance human capability in many ways. If artificial eyes can convert video to nerve signals, won't it be possible to use the same technique to superimpose computer-generated information in front of one's field of view?[61]

This capability will have extraordinary commercial applications from medical advances. These advances will help restore patients with damaged neural, audio, and visual systems as well as enable individuals to achieve the "ultimate virtual reality trip."[62]

### Visualization and Mental Imaging

This second broad category encompasses a realm of the cyberspace essential to the concept. Developing technologies are based around the idea of virtual projection systems that evolve into holographic image projection. The National Center for Supercomputing Applications Virtual Reality Laboratory "is a research facility engaged in the exploration of new methods of visualizing an interfacing with scientific data and simulations."[63] To further their objectives, they have created the CAVE a "surround-screen surround-sound, projection-based virtual reality system."[64] Multiple participants can enter the CAVE and interact by wearing stereo glasses rather than a helmet. "The CAVE can be coupled to remote data sources, super computers and scientific instruments via high-speed networks."[65] The NWV Information Technology Panel considers significant virtual reality advancements in the next 10 to 20 years. However, the display mechanism will primarily involve a helmet.

Commercial applications are easy to envision, witness the growing entertainment market for virtual reality games. This appears to be the next step from video teleconferencing. Another useful application will be for training systems—especially simulations.[66] This has wide commercial applications, especially as future systems will require such high-knowledge levels to use them as transportation and manufacturing.

A more specific military application of this type of technology is the DOD simulation network (SimNet). This capability allows a simulator to emulate a battlefield precisely. Trainees sit in their own aircraft or tank simulator and are able to "view" the battlefield from their own perspective. "Army tankers in trainers in Fort Knox can look out of their sites and see the same location—only from each of their individual perspectives. Air Force pilots in California can 'fly' missions . . . at the same time."[67]

A combination of brain processes and visual imaging already has been developed in the laboratory. The California Institute of Technology has developed an energy efficient computer chip which emulates the analog thinking of the human brain. It is specifically modeled on the construction of the human brain, specifically the cerebral cortex.[68] When this capability is fully mature, this chip could provide the baseline for a brain implant hooked to the sensory segments of the brain, not just the eye.

## Bringing It All Together—The Nexus

While each technology area will progress at a unique rate, the challenge is to bring them together to reach their synergistic peak—the nexus (fig. 3-3).

### Collection

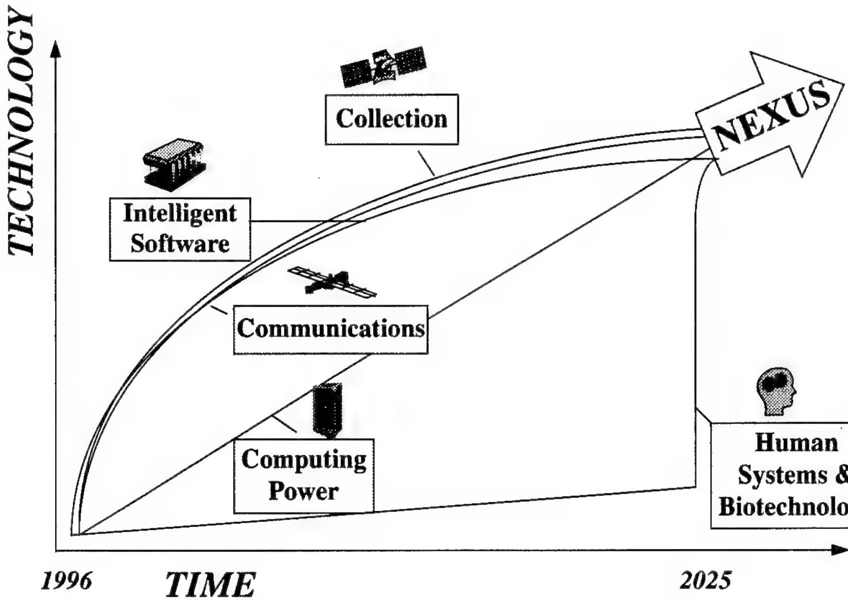
Collection capability will be complete when there is no want of information. The various constellations of permanent satellites complimented by the mini satellites will provide coverage of the entire world in every spectrum. Collection development should continue to grow until about 2015, when the complete link between the small satellites and the permanent constellations should be seamless, and the small satellite development will be commensurate with the requirements.[69]

### Communications

Communications capacity will peak when the entire globe is accessible at all times and there is absolutely no restriction on the size or type of transmission available to the customer. The web of commercial, government, and military networks will be seamless, and only the speed of light will delay information movement. There is much effort underway, both in the commercial and military sector, to achieve this connectivity. Development of new systems and new capabilities should reach this goal by 2010.[70]

### Computing Power

Computing power will continue to grow in capacity, doubling every 18 months for the near term.[71] As noted, analysts have




**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 3-3. Development Lines for System Elements**

frequently thought the silicon chip had reached its capacity, then discovered through increased micronization that more capacity could be obtained. However, most analysts believe that the silicon chip will hit its peak between 2015 and 2020.[72] If true, R&D efforts will continue to search for other media to store and process data.

**Intelligent Software**

Intelligent software is increasing in its availability but has yet to fully meet the requirements of the Cyber Situation. More effort is required to allow full capability of intelligent systems and bring that technology to bear on an advanced decision tool. Current intelligent software development is not well articulated, and the specific capability of the software is left to systems designers and engineers meeting the demands of a specific program.[73] Thus, much of the development of intelligent systems is linear and relates only to the requirements of a specific program. Such a design is not conducive to interaction and broader application.

**Human Systems and Biotechnology**

This area requires the most work to achieve the Cyber Situation. Work is expected to continue at a modest pace until a breakthrough in the this technology is achieved.[74] Like many advanced research areas, work here will require one big leap over a single chasm. In this case, the chasm is understanding the way information is formatted in the brain and how it is used. Once this chasm is achieved, progress in human computer interaction will grow exponentially and quickly catch up with the other technology areas.

By 2025 the five technology areas will be effectively linked to develop the Cyber Situation to enable commanders to achieve information dominance. The next chapter describes the Cyber Situation system, its components, and how it meets the attributes of the OODA Loop tasks.

**Notes**

1. Widnall and Fogleman, 11.
2. John L. Peterson, *The Road to 2015: Profiles of the Future* (Corte Madera, Calif.: Waite Group Press, 1994), 288. Peterson states, "Wild cards have a low probability of occurrence but a very high impact."
3. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the information applications volume, 15 December 1995), 68.
4. "New World Vistas" (unpublished draft, the human systems and biotechnology volume, 15 December 1995), 8.
5. Army Space Institute, *Theater Air Campaign Studies*, vol. 8, *Space Support in Mid-Intensity Conflict* (Maxwell AFB, Ala.: Air University Press, 1995), 306–9.
6. Ibid., 308.
7. "New World Vistas" (unpublished draft, the information technology volume, 15 December 1995), 85.
8. Nicholas Negroponte, *Being Digital* (New York: Vintage Books, 1995), 35–36.
9. Lt Col Henry Baird et al., "Spacelift" (Unpublished ***2025*** research paper, Air University, Maxwell AFB, Ala., April 1996); ***2025*** Concept, No. 900552, "On-demand Tactical Recce Satellite Constellation," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).
10. Numerous ***2025*** Concepts dealt with this technology to include: Nos. 900272, 900280, 900438, 900517, and 900604.
11. Lt Col Bruce Carmichael et al., "StrikeStar 2025" (Unpublished ***2025*** research paper, Air University, Maxwell AFB, Ala., April 1996), 94–95. Particularly, the appendix describes the historical reliability problems with UAV.
12. Alvin and Heidi Toffler, *War and Anti War* (New York: Warner Books, 1993), 90–91.
13. Negroponte, 21–36.
14. "New World Vistas" (unpublished draft, the information applications volume), 32–46.
15. A senior US Air Force policymaker lecture given to the ***2025*** Study Group under the promise of nonattribution
16. Aleksandar Kolarov and Joseph Hui, "Least Cost Routing in Multiple-Service Networks: Part II," On-line, Internet, September 1995, available from http://www.research.att.com/hgs/infocom95/program.html.
17. Negroponte, 211.
18. "New World Vistas" (unpublished draft, the information technology volume), C-3.
19. There are several different authentication technologies. The retinal (eye) scanner is currently used at Falcon AFB, Colorado.
20. Makoto Takano and Katsumi Fujita, "Multilevel Network Management by Means of System Identification," On-line, Internet, September 1995 available from http://www.research.att.com/hgs/infocom95/program.html.
21. Charles Kalmanek and K. G. Ramakrighnan, Third International Telecommunications Symposium, "On-line Routing for Virtual Private Networks," On-line, Internet, September1995, available from http://www.research.att.com/hgs/infocom95/program.html; Lt Col James McMillan, Air Force Liaison to National Security Agency, telephone interview by Maj Scott Bethel, 26 February 1996. MLS has been a long-standing DOD problem both in the US only (collateral versus SCI) and in releasing data to foreign nationals. The main problem is with data at different classification levels using the same communication architecture: how to prevent inadvertent or targeted database access at a higher classification level through lower channels.
22. "New World Vistas" (unpublished draft, the information applications volume), 52.
23. Institute for National Strategic Studies, *Strategic Assessment 1995: US Security Challenges in Transition* (Washington, D. C.: National Defense University Press, November 1994), 151.
24. "New World Vistas" (unpublished draft, the information technology volume), 1, 87–90.
25. "New World Vistas" (unpublished draft, the information technology volume), 87.
26. Patterson, 51.
27. Clarence A. Robinson, "Molecular Biology Computation Captures International Research," *Signal* 50, no. 6 (February 1996): 17–21; Thomas A. Bass, "Gene Genie," *Wired*, August 1995, 114–17, 164–68.
28. Robinson, 21.
29. Demetri Psaltis and Fai Mok, "Holographic Memories," *Scientific American* 273, no. 5 (November 1995): 70–76.
30. "New World Vistas" (unpublished draft, the information technology volume), 24. This document suggests "the communications laser will replace the microprocessor as the key enabling technology shaping the personal computer industry."
31. Ibid., 29. The document also suggests battery performance may be a limiting factor.
32. Advanced Research Program Agency, "The SISTO Solution: Intelligent Software Systems," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Solution.hmtl. SISTO is the Software and Intelligent Systems Office of the Advanced Research Program Agency.
33. Ibid.
34. Advanced Research Program Agency, "Intelligent Systems," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Intel_Thrust.html.
35. Oscar Firschein and Thomas Strat, "Image Understanding Program," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Image.html.
36. Ibid.
37. David Gunning, "Intelligent Integration of Information (I3)," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/I3.html.
38. Ibid.

39. "New World Vistas" (unpublished draft, the information technology volume), 38–44.

40. Ibid., 13.

41. Dr Tom Garvey, "Planning and Decision Aids Program," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/PDA.html.

42. Ibid.

43. "New World Vistas" (unpublished draft, the information technology volume), 13.

44. Allen Sears and Robert Neches, "Human Computer Interaction Program," On-line, Internet, 23 July 1995, available from http://www.arpa.mil/sisto/HCI.html.

45. "New World Vistas" (unpublished draft, the information technology volume), 37.

46. Ibid., 24.

47. Peter Thomas, "Thought Control," *New Scientist* 149, no. 2020 (9 March 1996): 39. The University of Utah has done significant work to map the brain. Through a series of some 100 sensors implanted in the brain, this team effectively mapped the parts of the brain that see and hear. Their focus was to reformat information to restore sight to the blind. They reported limited success as some of their research subjects claim to "see" words in their mind while reading them in Braille.

48. Peterson, 293.

49. Henry Petroski, *To Engineer Is Human* (Chicago: University of Chicago Press, 1989), 216.

50. Craig A. Rogers, "Intelligent Materials," *Scientific American* 273, no. 3 (September 1995): 123.

51. Ibid., 124.

52. Thomas, 38–42.

53. Ivan Amato, "Animating the Material World," *Science* 225 (17 January 1996): 284–86.

54. Thomas, 40.

55. Petroski, 211.

56. Thomas, 39; "New World Vistas" (unpublished draft, the human systems and biotechnology volume), F-1.

57. "New World Vistas" (unpublished draft, the human systems and biotechnology volume), F-2.

58. Thomas, 40.

59. Ibid., 41.

60. Negroponte, 128.

61. Peterson, 63.

62. Ibid., 41.

63. Bill Sherman, "NCSA Virtual Reality Lab & CAVE," On-line, Internet, 18 February 1996, available from http://www.ncsa.uiuc.edu/VR/VR.html. The laboratory is located at the University of Illinois at Urbana-Champaign.

64. NCSA VRL, Electronic Visualization Lab, University of Illinois at Chicago, "The CAVE: A Virtual Reality Theater," On-line, Internet, 18 February1996, available from http://www.ncsa.uiuc.edu/EVL/docs/html/CAVE.html.

65. Ibid.

66. "New World Vistas" (unpublished draft, the information technology volume), C-6–C-7.

67. Peterson, 46.

68. Ibid., 32.

69. A senior US Air Force policymaker lecture given to the ***2025*** Study under the promise of nonattribution.

70. George I. Zysman, "Wireless Networks," *Scientific American* 273, no. 3 (September 1995): 51.

71. Negroponte, 64; Rogers, 122.

72. Negroponte, 64; Rogers, 124.

73. "New World Vistas" (unpublished draft, the information technology volume), 38.

74. Thomas, 41.

# Chapter 4

# System Description

The vast array of technologies, concepts, and innovations in the previous chapter described the pieces that must be integrated to form the "Cyber Situation Vision." As seen in figure 4-1, the Cyber Situation Vision provides a commander with an "eye to see" all within a given battlespace.[1]

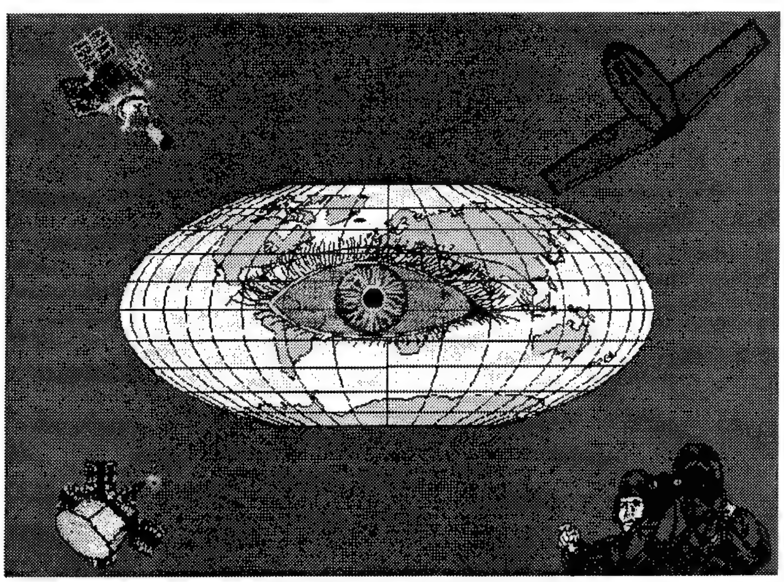
## Cyber Situation Components

The Cyber Situation is the integration of the entire OODA Loop Cycle under the control of commanders, decision makers, and analysts. Supporting components include all-source information collectors, archival databases, the Information Integration Center (IIC), a microscopic chip implanted in the user's brain,[2] and a wide range of lethal and nonlethal weapons (fig. 4-2).

This chapter first describes the five Cyber Situation system components which could result from technological advances. Next, it relates these advances to each system component (table 5). It then describes Cyber Situation integration and focuses on developing the two key components to achieve information dominance and seamless interface between the users and systems—the IIC and microscopic chip (the third and forth components). The first two components (information collectors and databases) provide the inputs, while the fifth component (lethal and nonlethal weapons) is the link to the act—the end product that results from a system that provides battlespace awareness. Finally, this chapter compares and evaluates the system capabilities with the requirements discussed in chapter 2.

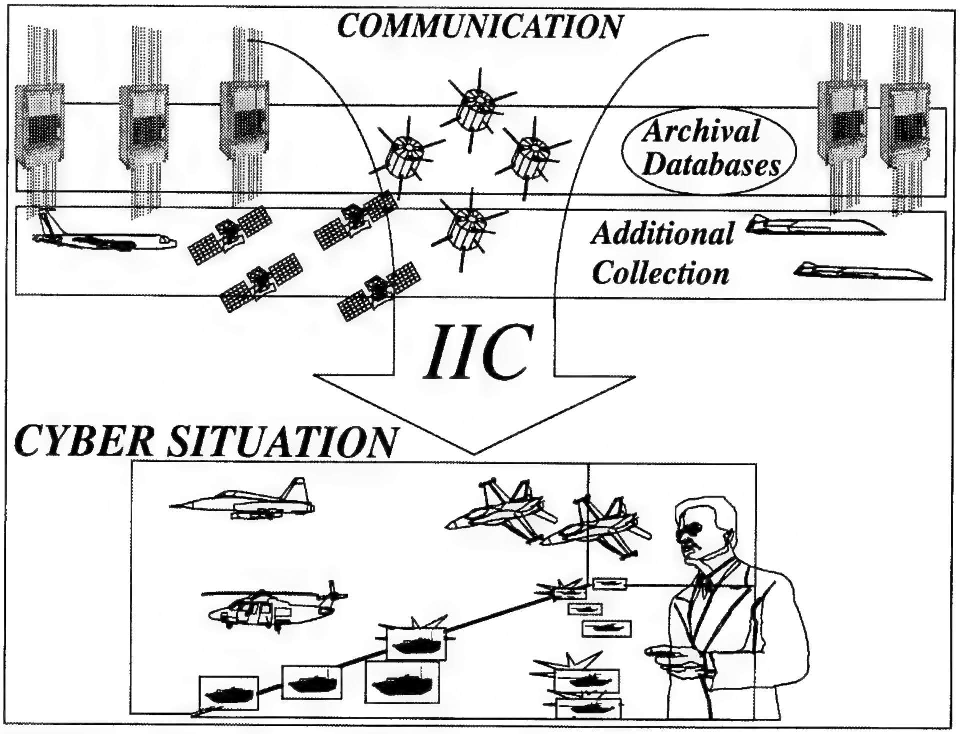
### All-Source Information Collectors

All-source information collectors will transmit raw data to the IIC, discussed



**Source:** MSgt Gordon Morrison, CADRE/EDECT, Gunter Annex, Alabama

**Figure 4-1. Cyber Situation Vision: "Eye" See Everything**




**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 4-2. Cyber Situation Components**

below. The collectors are linked by way of high-speed relay and dissemination systems. The collection platforms, in air and space, will be numerous and flexible.

**Archival Databases**

Archival databases will be used for historical analysis and to fill gaps if the information is not available for collection.

**Table 5**

**Technology Areas versus Cyber Situation Components**

| | TECHNOLOGY AREAS | | | | |
|---|---|---|---|---|---|
| **Cyber Situation Component** | **Collection Platform** | **Communications Infrastructure** | **Computing Power** | **Intelligent Software** | **Human Systems & Biotechnology** |
| All-Source Information Collectors | X | X | X | X | |
| Archival Databases | X | X | | | |
| IIC | | X | X | X | X |
| Implanted Microscopic Chip | | X | X | X | X |
| Lethal & Nonlethal Weapons | | X | X | | |

Much of the archival data will be resident in the GII, while secured permanent ground stations will store classified data.

### IIC

The IIC is a constellation of integration or "smart" satellites that receives all-source information. Within the IIC, resident intelligent software will run decision support tools, correlate and fuse data into useful information, identify inconsistencies and information gaps, and task collectors to seek data to fill information gaps.

### Implanted Microscopic Chip

The implanted microscopic brain chip[3] performs two functions. First, it links the individual to the IIC, creating a seamless interface between the user and the information resources (in-time collection data and archival databases). In essence, the chip relays the processed information from the IIC to the user. Second, the chip creates a computer-generated mental visualization based upon the user's request. The visualization encompasses the individual and allows the user to place himself into the selected battlespace.

Why the Implanted Microscopic Chip? While other methods such as specially configured rooms, special helmets, or sunglasses may be used to interface the user with the IIC, the microscopic chip is the most viable. Two real operational concerns support the use of implanted chips and argue against larger "physical" entities to access the Cyber Situation.

First, future operations will demand a highly flexible and mobile force that is ready at moment's notice to employ aerospace power. The chip will give these forces the ability to communicate, visualize, and prosecute military operations. Having to manage and deploy a "physical" platform or room hampers mobility and delays time-sensitive operations. US aerospace forces must be prepared to fight or to conduct mobility or special operations anywhere in the world on extremely short notice, although some of these operations may be staged directly from the continental United States.[4]

Second, a physical entity creates a target vulnerable to enemy attack or sabotage. A highly mobile information operations center created with the chip-IIC interface makes it much more elusive to enemy attack. These reasons argue against a larger physical entity for the Cyber Situation.

While this is a reasonable portability rationale for the use of chip, some may wonder, "Why not use special sunglasses or helmets?" The answer is simple. An implanted microscopic chip does not require security measures to verify whether the right person is connected to the IIC, whereas a room, helmet, or sunglasses requires additional time-consuming access control mechanisms to verify an individual's identity and level of control within the Cyber Situation.

Further, survey any group of commanders, decision makers, or other military personnel if they enjoy carrying a beeper or "brick" at all times. Likely, few like to carry a piece of equipment. Now, imagine having to maintain a critical instrument that allows an individual to access the Cyber Situation, and thus control the US military forces. Clearly, this is not an enviable position, since the individual may misplace or lose the helmet or sunglasses, or worse yet, the enemy may steal or destroy it. These are unnecessary burdens.

### Ethical and Public Relations Issues

Implanting "things" in people raises ethical and public relations issues.[5] While these concerns may be founded on today's thinking, in 2025 they may not be as alarming. We already are evolving toward technology implanting. For example, the military currently requires its members to receive mandatory injections of biological organisms (i.e., the flu shot). In the civilian world, people receive mechanical hearts and other organs. Society has come to accept most of these implants as a fact of life. By 2025 it is possible medical technology will

have nerve chips that allow amputees to control artificial limbs or eye chips that allow the blind to see.[6] The civilian populace will likely accept an implanted microscopic chip that allows military members to defend vital national interests. Further, the US military will continue to be a volunteer force that will freely accept the chip because it is a tool to control technology and not as a tool to control the human.

### Lethal and Nonlethal Weapons

A wide range of lethal and nonlethal weapons will be linked to the IIC, allowing authorized users to directly employ these weapons. A user's authority to employ weapons will depend on the person's position, responsibility, and rank.

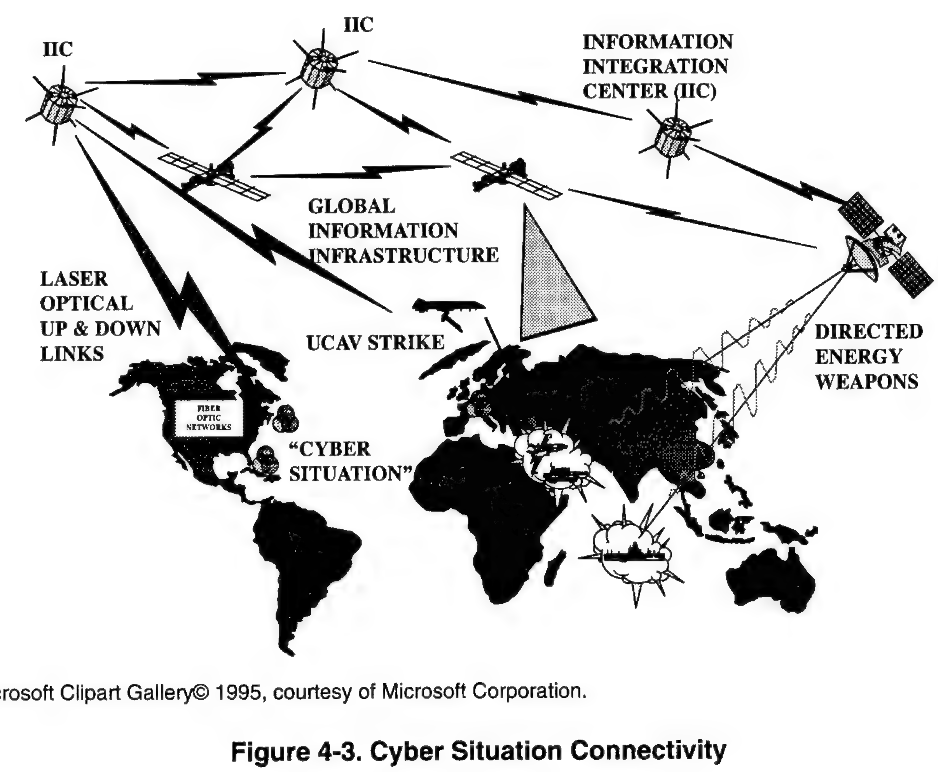
## Putting It Together

The Cyber Situation is not a traditional operations or command and control center. Not a physical infrastructure, it consists of many components geographically dispersed, redundant, and networked (fig. 4-3). When an authorized individual needs situational updates and analyses, the user will link to an IIC satellite by way of the implanted chip.

The Cyber Situation is applicable at all levels of war. At the strategic and operational levels, it provides the user the capability to monitor global activity, analyze developing situations, monitor and control the battlespace, assess battle damage, and conduct reconstitutions. Tactically, the Cyber Situation offers battlespace situational awareness by conveying in-time enemy and friendly information. At all levels, the Cyber Situation gives decision makers and analysts the ability to coordinate, respond, and execute battlespace operations.

## Measures of Merit

Thus far, this paper has shown how the five key technology areas (collection platforms, communications architecture and dissemination systems, computer-




**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 4-3. Cyber Situation Connectivity**

processing power, intelligent software, and human systems and biotechnology) will logically synergize by 2025 to realize the Cyber Situation vision to enable information dominance. The paper asserts that to achieve this vision, technology must allow military commanders to integrate the functions of the OODA Loop and enable the military commander to control momentum. Whether Cyber Situation meets the goal is best answered by evaluating the Cyber Situation against the measures of merit developed in chapter 2. The measures of merit encompasses a list OODA Loop tasks with associated attributes that describes how the task should be performed.

## Observe Tasks

The IIC component of the Cyber Situation provides the avenue to meet the attributes of this "see the battlespace" task (table 6). The IIC includes an inherent capability to fuse, correlate, and deconflict available all-source information. Further, built into the system description is the ability to identify information gaps. Links allow the IIC to task collection assets to fill information gaps and deconflict contradictory information. If the collection assets are not able to obtain further information, the IIC uses historical archival databases to fill in gaps. Accordingly, the IIC lets the user know the picture's reliability.

Within the Cyber Situation vision, the ability to maintain a "mobile" battlespace picture is perhaps its most significant characteristic (table 7). The use of the implanted microscopic chip linked to the IIC allows the user to pull a computer-generated mental visualization of the desired battlespace anytime, anywhere. Further, the user is not confined to any physical room or platform to enter the Cyber Situation system, making it impenetrable. Even more advantageous, the user has no worry of losing or having someone steal the microchip because it is not

**Table 6**

**See the Battlespace**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Fused, integrated, and deconflicted view of the desired battlespace | Yes |
| • Sum of all possible information sources | Yes |
| • System identification of information gaps and subsequent collection of missing information | Yes |

**Table 7**

**Maintain Mobile Battlespace View**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Able to pull updated view anytime, anywhere | Yes |
| • Easily deployable and transportable with user | Yes |

**Table 8**

**Universal Access to Battlespace View**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Able to tailor picture for relevant AOR, missions, and tasks | Yes |
| • Many able to see the same battlespace picture | Yes |

a detached physical entity that requires accounting and protection.

The IIC allows virtually unlimited number of users to simultaneously access the system because it operates on the user-pull concept. This system's characteristic allows multiple users to access the same battlespace picture and create a "cyber conference" within the Cyber Situation system (table 8). Further, IIC's resident intelligent software, coupled with taskings transmitted by way of the chip, allows the user to define the battlespace picture dimensions. This process enables the user to tailor the battlespace computer-generated mental visualization to the relevant area of responsibility (AOR), mission, and tasking to prosecute military operations.

## Orient Tasks

Since the IIC uses the most current data to create battlespace picture, the user's mental visualization will be the most up-to-date information available. As with the previous task, IIC resident intelligent software, coupled with taskings transmitted by way of the microscopic chip, allows the user to define the battlespace picture dimensions (table 9).

Commanders using the Cyber Situation system receive battlespace information that is less biased than the same information when conducted by human processing, interpretation, and presentation. Further, the system minimizes the need for the commanders to mentally reconstruct the information presented by analysts and briefers (table 10). If the users sense the battlespace picture does not logically compute, or if they just want additional information, they may request the IIC confirm the situation. The IIC then tasks additional collection assets to seek further data and searches the archival database for further analysis.

## Decide Tasks

The IIC acts both as a receiver and as a transmitter. As a receiver, it accepts data

**Table 9**

**Tailor View of the Battlespace**

| ATTRIBUTES | YES OR NO |
|---|---|
| • In-time view of the battlespace | Yes |
| • Able to define dimensions and locations of battlespace | Yes |

**Table 10**

**Comprehend the Battlespace View**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Eliminate biased inputs from one person to another[7] | Yes |
| • Eliminate need for mental picture based on another's biases | Yes |
| • Able to query for further information and receive in-time answers | Yes |

**Table 11**

**Decide What Is Important and What May Require Action**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Decision support tool in transmitter and receiver to filter, sort, and prioritize | Yes |
| • Prompts user of significant events for monitoring and action | Yes |

from collection assets, users' queries for additional information, and commander's orders to employ remote weapons, space-based lasers, and UCAV. As a transmitter, it responds to users' information requests, prompts users of significant events, tasks collection assets, and relays orders from the users to space-based lasers and UCAV to employ weapons. Within the transmitter and receiver components of the IIC, intelligent software automatically filters, sorts, and prioritizes data for processing and fusing. Ultimately, the IIC prompts the user of significant event and the user decides whether action is required for the situation (table 11).

As a decision aid, the Cyber Situation system allows users to model outcomes of potential actions and inactions to determine the optimum course of action (table 12). The modeling process lets the user best apply precision force at the least risk to friendly forces to achieve military objectives.

**Act Tasks**

The IIC will be linked to such lethal and nonlethal assets as space-based laser and various UAV. The authorized user will have immediate access to these assets to rectify an undesirable situation. Precision-force assets could allow users to optimize weapons to achieve one shot and one kill capability (table 13).

Upon taskings from authorized users to employ space-based laser assets and UAV, the IIC also will task collection assets to accumulate data from the target. The IIC then processes and analyzes the data to provide in-time feedback to the users (table 14). It also recommends additional actions if the target is not satisfactorily affected.

The Cyber Situation system could change dramatically how commanders process information and take action or cycle information through the OODA Loop. To be effective, the Cyber Situation system must be optimized to minimize vulnerabilities.

**Table 12**

**Determine Action Required to Rectify Undesirable Situation**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Model effectiveness of potential actions and inactions with in-time feedback | Yes |
| • Optimize application of precision force | Yes |
| • Ensure least risk to friendly forces | Yes |

**Table 13**

**Immediate Access to Assets to Rectify Undesirable Situation**

| ATTRIBUTES | YES OR NO |
|---|---|
| • Ready lethal capabilities for employment | Yes |
| • Ready nonlethal capabilities for employment | Yes |
| • One shot, one kill capability | Yes |

**Table 14**

**Feedback on Actions Taken and Inactions**

| ATTRIBUTES | YES OR NO |
|---|---|
| • See in-time mission results | Yes |
| • System recommends additional action or inaction | Yes |

The next chapter reviews those potential weaknesses and countermeasures.

## Notes

1. Special thanks to MSgt Gordon Morrison, CADRE/EDECT, The Extension Course Institute, Air University, Gunter Annex, Maxwell AFB, Ala., for his depiction and creation of the "Cyber Situation," 25 March 1996.

2. ***2025*** Concept, No. 900702, "Implanted Tactical Information Display," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

3. ***2025*** Concept, No. 200169, ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

4. Peter Grier, "New World Vistas," *Air Force Magazine*, March 1996, 20.

5. Anonymous assessor comments on ***2025*** Concept Identification 900702, ***2025*** Concept Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

6. John L. Peterson, *The Road to 2015* (Corte Madera, Calif.: Waite Group Press, 1994), 63.

7. Col Joseph A. Engelbrecht, Jr., ***2025*** research director and professor of Conflict and Change, Air War College, Maxwell AFB, Ala., personal interview with Major Whitehead, 17 March 1996. Colonel Engelbrecht explains that "Eliminating human biases may be impossible. Since the decision is reserved for the commander or decision maker, the potential for bias may always remain. On the other hand, communication theory and prospect theory from psychology suggest the importance of how the message is framed. Framing the message can set up a bias in the human receiver. Thus, potentially, technology should be able to help by providing alternate frames or contexts or highlighting a perspective highly relevant for the data and circumstance. While designing the technology to meet the challenge may be difficult, if it is not pursued humans may be trapped in a noisy cacophony of inputs that become screened or skewed simply because little progress has been made in human-machine interfaces."

# Chapter 5

# Vulnerabilities and Countermeasures

Identifying vulnerabilities of the Cyber Situation and its associated components, then developing potential countermeasures, leads to additional features and attributes that should be integrated into the Cyber Situation requirement list. This chapter begins by identifying vulnerabilities of the Cyber Situation and then states possible countermeasures that eliminate the vulnerabilities.

## Vulnerabilities

Numerous vulnerabilities of the Cyber Situation system and its associated components exist. The vulnerabilities naturally fall into three primary categories, man-made threats (space debris and offensive weapons), environmental threats (meteors, asteroids, and radiation), and human threats (capture, defection, and espionage).

The first threat area, man-made, generally designed to destroy, disable, or degrade its targets. The effects may be either permanent or temporary and may consist of hard and soft attacks. Adversaries achieve "hard kills" by physical destruction of the Cyber Situation through destruction of system components. Specific methods of attack may include antisatellite weapons, electromagetic pulse (EMP) weapons, and nuclear detonation devices. Conversely, "soft kills" attack the internal logic within the operating capability. An example of soft attack is syntactic attacks of the operating logic inside the IIC and collection computers. The resultant loss or decrease in effectiveness, if not replaced in a timely manner, will have dire consequences on military operations.

Less obvious military vulnerabilities come from the second threat area, environmental, which includes solid debris that disintegrated or decomposed from celestial or man-made materials. Expert views differ as to whether asteroids really pose enough of a problem to develop defenses against the threat.[1] Nevertheless, the threat results from the kinetic energy produced by the projectiles roving through space at rapid velocities. Even the smallest fragments pose a potential threat to IIC and satellite collectors. Other environmental threats include radiation and charged particles which come primarily from the sun. These "space weather" effects may be gradual or instantaneous. These effects are usually difficult to detect until after catastrophic failure.

The last threat area involves people and can be subdivided into two categories: the capture of our people implanted with the microscopic chip and the espionage and defection to the enemy side. All three categories of threats (man-made, environmental, and people) will destroy, disable, or degrade our ability to perform tasks that support our core capability of information dominance.

## Countermeasures

Countermeasures include both passive and active activities that can be used against a variety of threats. The following paragraphs describe several activities and discusses their effect on vulnerabilities.

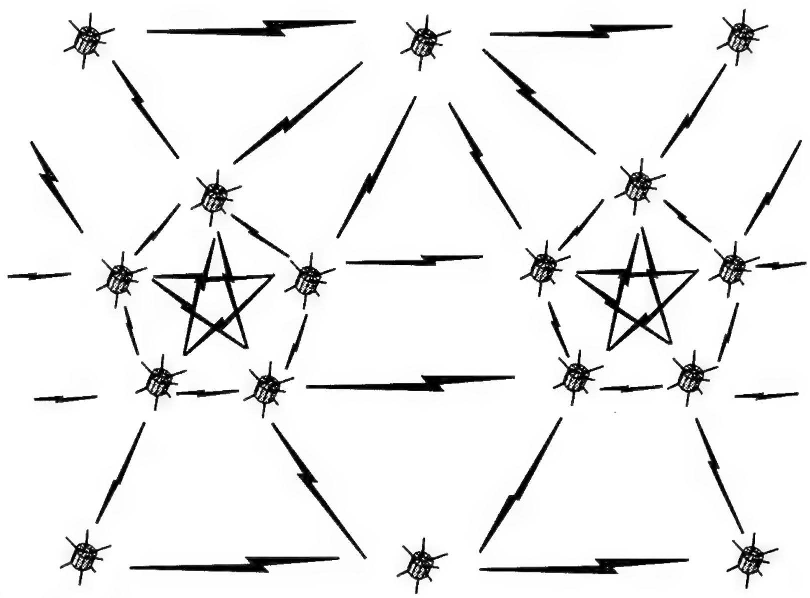
### Distributed System Architecture

The defensive goal behind the use of a distributed system architecture for the IIC is to deny the enemy a center of gravity to attack. In other words, use of this type of architecture will deny the enemy the IIC as a target that if destroyed "would cause a system failure or cascading deterioration within the system," allowing the enemy to achieve its objective.[2]

The network of IIC satellites are interconnected using the "star" interconnectivity, which has lines radiating out from each satellite to other satellites (fig. 5-1).[3] Essentially, the satellite constellation forms a "mesh" over the earth's atmosphere.[4] The interconnected mesh allows for graceful degradation so that if the enemy physically destroys a percentage of the IIC, it does not lead to a total loss of effectiveness. Further, because of the interconnectivity, the mesh knows to compensate and fill in the gaps created by the destruction. The mesh has no center of gravity so if the adversary wants to defeat the IIC, it must be destroyed in total.[5]

electronics and miniaturization have given impetus to smallsat concepts that weigh approximately 20 to 30 pounds and are smaller than shoe boxes.[6]

The qualities of redundancy, miniaturization, and low cost will describe future components that make up the IIC. The "small and the many" concept results in a system that is redundant and difficult to completely destroy.[7] Like the IIC concept, this concept allows the enemy no center of gravity to target, therefore, no single point of failure. Further, even if adversaries destroy a portion of the network, it will still survive and operate.



**Source:** Microsoft Clipart Gallery© 1995, courtesy of Microsoft Corporation.

**Figure 5-1. Information Integration Center Interconnectivity**

### The "Small and the Many"

Components that feed information and support the IIC will be composed of many inexpensive sensors, emitters, microsats, and miniprojectiles. Similarly, the IIC mesh also consists of many small satellites (minisats) that are inexpensive and easy to launch. Current minisat development and designs produced satellites that weigh several hundred pounds and measure about three cubic feet. Recent advancements in

### "Smart" System

Inherent in the IIC system is the built-in capability to fuse, correlate, and, most importantly, *deconflict* contradictory inputs and data points. Therefore, when adversaries attempt information warfare by injecting false statements (syntactic attacks) into the logic tree, the computing system within the IIC will recognize the inconsistencies and deconflict them. The IIC consists of a body of knowledge and an

"ability to learn" to know when a possible conclusion is invalid or simply does not make sense.[8] When the IIC detects inconsistencies, it will seek additional data either to validate or invalidate its own conclusions.

If the individual attempts to enter a particular Cyber Situation when the IIC concludes there are invalid resolutions, it will inform the user of the potentially false inputs and its attempt to resolve the data confliction. If the individual desires, the IIC will show the conflicting data and why a possible conclusion is invalid.

**Optical Computing**

Much research continues in this area of optical networks to transmit, receive, and store information. The technology appears promising and at minimum would seem a plausible radiation defense.[9] The use of optical computing in the IIC (to receive inputs from other collectors and users, to respond to users' requests to develop the Cyber Situation picture, or to task lethal and nonlethal assets) would serve as protection against radiation threats. Radiation attacks systems that use electrons to transmit data. Since optical computing employs photons instead of electrons, these photons render optical computing systems safe from EMP threats.

**Low Earth Orbit**

Employing the IIC in a low earth orbit (LEO) will minimize exposure to environmental radiations. Compared to other orbits, the LEO naturally is exposed to lower levels of radiation. By contrast, medium orbits have the highest levels of radiation, primarily caused by the Van Allen Radiation Belts, while at the geosynchronous orbit, the radiation level is higher than the low-earth orbit but lower than the medium orbit.[10]

**Internal Deactivation**

If captured by the enemy, users with the implanted microscopic chip may self-deactivate the chip and render it useless. Further, the chip disintegrates and cannot be extracted by the enemy for reverse engineering or for adversarial reasons.

**External Deactivation**

When faced with the disturbing events of espionage and defections of friendly users to the enemy side, the IIC is engineered with the capability to deactivate and disintegrate the offender's implanted chips. The highest level commanders within the US military have the authority to access the IIC and order the system to deactivate the defectors' chips the next time they try to activate the Cyber Situation.

**"Zap" Attack**

"Zap" attack relies on the decision-support technology built into the IIC and its link to space-based laser weapons. As individual satellites within the IIC network sense an object (man-made or environmental) moving toward its network, the IIC will compute the object's directional objective, velocity and acceleration, and Doppler shift to determine whether it is a threat. If the decision is affirmative, the IIC will instruct the nearest space-based laser weapon to destroy the object and eliminate the threat to the IIC system.

**"Mutual Dependence"**

Once implanted, the microscopic chip will operate only when the individual is alive because the chip creates mutual dependence on its host. In the unfortunate circumstance where a Cyber Situation user dies, the implanted microscopic chip becomes nonfunctional and disintegrates. This operational dependence of the chip upon its host prevents adversaries from using a chip from a deceased war fighter.

## Summary

Table 15 presents a list of threat categories and associated countermeasures that will address each type of threat. Note that each

**Table 15**

**Countermeasures versus Threats**

| | THREAT | | |
|---|---|---|---|
| **COUNTERMEASURE** | **MAN-MADE** | **ENVIRONMENTAL** | **HUMAN** |
| Distributed System Architecture | X | X | |
| "Small and the Many" | X | X | |
| "Smart" System | X | | X |
| Optical Computing | X | X | |
| Low Earth Orbit | | X | |
| Internal Deactivation | | | X |
| External Deactivation | | | X |
| "Zap" Attack | X | X | |
| "Mutual Dependence" | X | | X |

countermeasure may be effective against more that one type of threat.

Though numerous vulnerabilities exist with the Cyber Situation, by 2025 effective countermeasures likely will be integrated into the system. Well-developed measures to defeat these man-made, environmental, or human threats can make the Cyber Situation more effective to the war fighter. Chapter 6 goes beyond threats and countermeasures and explores potential structure and doctrine changes required to achieve and take full advantage of the Cyber Situation.

**Notes**

1. Anonymous assessor comment on ***2025*** Paper Draft (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

2. Paul Moscarelli, *Strategic Structures Course Book*, vol. 2, *Operational Analysis: An Overview* (Maxwell AFB, Ala.: Air University Press, 1995), 522–23.

3. Negroponte, 33.

4. Martin C. Libicki, *The Mesh and the Net* (Washington, D. C.: National Defense University Press, 1994), 3. Libicki defines *mesh* as "the term applied to military applications—points to the holes; as information technology places a finer mesh atop the battlefield, more objects are caught in it."

5. Ibid., 33.

6. Air Force Scientific Advisory Board members, review and comments from ***2025*** Concept Briefings (Maxwell AFB, Ala.: Air War College/***2025***, 5 February 1996).

7. Ibid., 19–37.

8. Negroponte, 154–56.

9. Vincent W. S. Chan, "All-Optical Networks," *Scientific American* 273, no. 3 (September 1995): 57–58.

10. Michael J. Muolo, *Space Handbook: Space Analyst's Guide*, vol. 2 (Maxwell AFB, Ala.: Air University Press, December 1993), 13–14.

# Chapter 6

# Concept of Operations

*Today's breathtaking technological achievements notwithstanding, developing the concept of operations that incorporate new technologies and organizations to permit effective exploitation of new capabilities is even more critical than acquisition of the technologies themselves.*

—James R. Fitzsimonds
*Revolutions in Military Affairs*

This chapter discusses how the Cyber Situation will be implemented and expound on what capabilities the Cyber Situation offers to future war fighters.

Implementing the system will require dramatic changes to our present-day organizational structure and doctrine. No doubt some of these changes will appear radical and meet stiff resistance by individuals and institutions unconvinced of the merits the Cyber Situation has to offer to the defense efforts of United States military. History has shown those entities unable or unwilling to adapt to change have, at best, been left behind, and in the worst instances been eliminated as an entity.

To realize the full potential of the Cyber Situation, tomorrow's aerospace forces must devise dramatically different supporting organizations and doctrine in order to fully harvest these innovative new capabilities. As noted in previous chapters, the technology will be available in 2025; it will be the organization and command structures along with the doctrine and concept of operations (CONOP) that will form the second and third legs of the revolution in military affairs (RMA) triad.

## Future CONOP

War-fighting and conflict management in 2025 will apply the results of improved concepts and technology applications in the areas of surveillance and reconnaissance, command and control, and overall battle-space execution. As forecast in the 1994 SPACECAST 2020 study, "advances in surveillance and reconnaissance, particularly real-time 'sensor to shooter' to support 'one shot, one kill' technology, will be a necessity if future conflicts are to be supported by a society conditioned to 'quick wars' with high operational tempos, minimal casualties, and low collateral damage."[1] The Cyber Situation has the potential to be the harbinger of the revolution.

## Applications of the Cyber Situation

The Cyber Situation is ideally suited for the command, control, and execution of military operations across the spectrum of warfare from the selective release of nonlethal weapons to the full-scale assault of parallel war. In parallel war, aerospace forces simultaneously attack enemy centers of gravity across all levels of war (strategic, operational, and tactical) at rates faster than the enemy can react.[2]

Commanders always seek to control the throttle of the OODA Loop, operating faster or slowing the decision cycle of their foes. In past wars, tank commanders and fighter pilots always strove to get "inside the enemies OODA Loop." The difference in future conflicts will be the speed and scope of their decisions.

Parallel war requires large numbers of highly precise weapons directed against critical nodes. Additionally, they require a requisite level of detail on the enemy situation necessary for precision targeting. For these reasons yesterday's military commanders could not wage parallel war effectively. The Cyber Situation is ideal for conducting parallel war because it offers capabilities that fill both of these voids.

The Cyber Situation offers tomorrow's commanders an in-time view of the battlespace, exposing the enemy centers of gravity before his eyes. In 2025 operating at previously unheard of speeds will be a common feature of military engagement. Future warriors by way of the IIC will conduct Cyber Situations utilizing a whole new array of air and space sensors, UCAV, directed energy weapons, and highly mobile expeditionary forces. Operations will be controlled from Cyber Situations in continental US (CONUS) and instantaneously reach out and touch the enemy halfway around the globe.

A CONUS-based joint task force commander, for example, would have well exercised connectivity with combat units through Cyber Situations with CONUS-based stealth bombers, UCAV, and instantaneous access to space-based precision strike weapons. Imagine the psychological effect on the adversary who will be unable to predict where the next blow will fall and will be powerless to defend against it.

## Command Structure

The 2025 force structure and battlespace requirements will make obsolete traditional hierarchical command and control arrangements. Cyber Situation capabilities require greater decentralization through information technology, growth of distributed systems and establishment of virtual organizations.

> New information and communications technologies are shifting power to those with the most powerful computers and most effective sensors . . . at the same time, the punch packed by the individual soldier is increasing, eroding the role of field commanders and resulting in flatter command and control structures.[3]

The Cyber Situation allows greater emphasis to be placed on decisive decision making, precision engagement, high-speed and synchronized maneuver, agility, and enhanced command and control. The command structure will have freedom of operation within previously identified parameters much like the vaunted German decentralized, flexible command style known as *Auftragstaktik* (mission tactics). This method of battlefield command has enabled smaller forces to defeat much larger ones through a timely ability to seize the initiative and act according to "on the spot" judgment. The German breakout at Sedan, resulting in the fall of France in 1940 offers a familiar example of the successful employment of this flexible command philosophy.[4]

The war fighter must have access to a broad range of supporting weapons, improved mobility, survivability, and supportability—these changes that reflect a dramatically flattened command structure staffed by an extremely high caliber individual at every level. As the battlefield becomes less dense and more decentralized, the demands on small unit leaders increase. The flattened structure permits power to be defused and redistributed, often to subordinate actors. The overall impact is that the flow of information, and its associated awareness and knowledge, compels closed systems to open, eliminating many layers of the cumbersome and compartmented intelligence and analysis bureaucracy. The traditional emphasis on command and control will give way to an emphasis on consultation and control. This organizational structure permits the Cyber Situation to operate at maximum efficiency. It allows commanders at all levels to operate with greater latitude and autonomy as part of an integrated joint operation—a truly combined arms.

## Principles of War

The Cyber Situation will provide enormously enhanced capabilities and

opportunities for the war fighter, but it will not alter the fundamental principles of war—objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, and simplicity. These nine principles guide war fighting at all levels of warfare and have withstood the test of time and will endure in 2025 as the bedrock of US military doctrine.[5] The Cyber Situation optimizes the principles of offense, mass, and maneuver, enabling the commander to execute a wide array of precision weapons from CONUS across the spectrum of warfare at a single decisive point or a parallel attack against multiple critical nodes. The following section depicts the Cyber Situation in action in a hypothetical 2025 scenario.

## A Future World

(12 March 2025—1435 EST/2045Z) The persistent flashing blue light at the corner of his vision alerted the CJCS that the NMCC was initiating a category II ALERT, the blue code for International, Domestic. As the chairman made himself comfortable, he double-blinked rapidly to set in motion his Cyber Situation. As his computer-generated mental display command center whirled into being before his eyes, his mental display-mail—the message that started the ALERT—became operational. CINCSOUTH's image appeared and began briefing.

The government of Argentina was asking for help in conducting a hit on a narcoterrorist group hidden within a room in the center of the Zircon building, a 50-story skyscraper building in downtown Buenos Aires. The Argentina government is worried because the building also contains thousands of civilians unaware of the terrorists' presence. A moment's thought and the topographical detail map of Buenos Aires floats into view. As the CJCS studied the map from all angles, zeroing in on the Zircon building, the other major players "stepped" one by one into the "Cyber conference." The NCA, along with the unified CINCs, service chiefs, and State Department representatives all studied the unfolding three-dimensional schematics of the Zircon building within their own personal "cyberspace." Weather reports began to come in, indicating a storm raging off the coast in Tierra Del Fuego with winds NNE at 35 miles per hour. Light rain was falling in and around Buenos Aires. Now the CJCS moved into the "Cyber Situation" of the intelligence analyst that had been monitoring the situation. DNA and heat-sensing probes of the Zircon building were built into a three-dimensional map that pin-pointed the location of the terrorists on the 23d floor in the offices of the Argentina Spaceways Co. Two floors above, a local telecommunications company was hosting an AT&T International conference. Local police already had sealed off the outer sectors of the building.

After studying the situation, the CINCSOUTH then ordered the execution of Operation Red Ball One—Option 2, with the CJCS approval. At this point the CSAF took over the "Cyber Situation" and entered the "Cyber-space" of the ACC commander. Together, they reviewed the life-like images that appeared before them marking US Aerospace bases. Beside each image were the unit's designator, manning level, and current activity. For the execution of Red Ball One—Option 2, after consulting his crisis action staff, the ACC commander decided to precision drop three squads of Space Marines from a TC-4 Globemaster on to the roof of the Zircon building. The Cyber Situation now included the colonel in charge of the 3d Special Operations Group, the squadron commander of the Space Marines at Hurlburt Field, Florida, and the Globemaster wing commander at Eglin AFB, Florida. Together, they reviewed the prevailing weather conditions, where the wind and rain could affect operations. Next, they reviewed the computer-generated mental display schematics of the Zircon building, deciding where best to precision drop the squads, mapping out the ins and outs of the stairways and speed lifts of the building. Each of the three squad leaders of the Space Marines entered the "Cyber Situation" for a detailed briefing of the Zircon building's many exits and entries. They discussed the placement of portable force-field shields to isolate the floor and at what point the various nonlethal weapons would be used. One of the Marines suggested using an ultrahigh frequency wave burst as the best method to subdue the terrorists with the fewest losses. The TAV-4 pilot and crew, already part of the Cyber Situation, once more reviewed the weather, adjusted for winds, and with the squadrons aboard, launched.

The CINC and others watched the outcome of the operation in their "Cyber Situations," noting the success of the precision drop and the excellent execution of the Space Marines in avoiding detection by the terrorists, while keeping the civilians calm. The success of the frequency wave burst earned the suggesting Space Marine a merit promotion and the entire operation the Argentine government's heartfelt thanks.

**Notes**

1. SPACECAST 2020, "Leveraging the Infospace: Surveillance and Reconnaissance in 2020" (Maxwell AFB, Ala.: Air University Press, June 1994), 1.

2. Jeffrey R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala.: Air University Press, 1996), 6.

3. Institute for National Strategic Studies, *Strategic Assessment 1995: US Security Challenges in Transition* (Washington, D. C.: National Defense University Press, November 1994), 16.

4. Robert Allan Doughty, *The Breaking Point: Sedan and the Fall of France, 1940* (Hamden, Conn.: Archon Books, 1990), 3.

5. Joint War-fighting Center Doctrine Division, *War-fighting Vision 2010: A Framework For Change* (Langley AFB, Va.: 1 August 1995), 2.

# Chapter 7

# Investigation Recommendations

This chapter discusses areas of concerns requiring increased R&D and time investment. First, it articulates specific shortfalls and identifies commercial and military solutions. Second, it identifies broader issues that will develop with the overall implementation of the Cyber Situation.

Some elements of the Cyber Situation have progressed further in the development process than others. By 2025 the communications architecture will be sufficiently robust to support the Cyber Situation. This will occur because of significant commercial investment as the civilian sector's insatiable appetite for increasingly rapid access to data facilitates greater profit for those who provide it. The military will likely be an investment partner in communications advances.

Computer power will continue to progress, doubling about every 18 months until the turn of the century. Again, the commercial sector will take the lead with the military purchasing adequate computer power "off the shelf."

Current development in other areas is not as advanced and will therefore require greater emphasis to mature at a comparable rate. Intelligent software is becoming more commonplace and its application more widely implemented. However, currently available intelligent software has narrow application and is neither very complex nor does it possess suitable capacity. To achieve the military requirements of the Cyber Situation, allocation of R&D funding must continue to increase the pace of development in intelligent software applications.

Finally, 2025 intelligence collection requires technology advances in both computer power and intelligent software but currently is more affected by the developmental limitations in intelligent software. Commercially available intelligence software is proliferating and will augment products developed and managed by the military. However, development of small satellites, both capable of short duration intelligence gathering as well as the ability to cover communication gaps, will require the infusion of scarce military dollars to supplement private sector investment.

The following are other, broader issues that require attention. First, the developmental technologies required by the Cyber Situation must have a more effective linkage. Since each of the capability areas required by the Cyber Situation is developing on a separate path, the synergistic effect of combining these areas might better achieve the goal of complete OODA integration.

Second, research into the functions of the brain must be encouraged and accelerated. This is a new area for both the medical community and the military. The research effort must focus on the capacity and interface within the brain and how information is processed in going from raw input to final decision.

Third, social and cultural biases to a brain implanted decision tool must be overcome. The Cyber Situation is designed to assist, *not* control each decision maker. To fully exploit growing technology, cumbersome hardware and software requirements must be reduced to the simplicity and seamlessness of a chip implant. With that technology in hand, the Cyber Situation can become a reality.

# Chapter 8

# Conclusion

The Cyber Situation makes the entire OODA Loop available to the commander in one location. It provides observation through the collection platforms, the IIC, and the computer chip. It orients the user using the IIC, the archival databases, and the brain chip. These are neither new nor revolutionary capabilities provided to the commander. Senior decision makers throughout time have had access to the orient and observe portion of the OODA.

Where the Cyber Situation provides a unique orient and observe capability to the commander is the rapidity in which a decision maker has access to a complete picture. Before the Cyber Situation linked the collectors and analysis tools in one step, each event was accomplished singly. Collectors were tasked and controlled by one group and the analysis occurred elsewhere. The collected and analyzed information then had to be briefed or presented to the commander who applied his own analysis to the information and determine his own solution. This information could (and often did) come to the commander incomplete or with biases. The Cyber Situation cuts through the processing and provides the commander with an in-time picture from which he can observe and orient to an unbiased and a complete picture.

With the commander fully informed, the Cyber Situation helps with the decision process. The Cyber Situation is designed to be a *decision aid* not a *decision maker*. This none-too-subtle difference confirms that, as conceived, the capability resident in the Cyber Situation is designed to facilitate the best possible decision from a human, who will always be in the loop. Options available to commanders for any situation will be clearly displayed and evident to them; they can select one or seek additional information from the Cyber Situation before proceeding.

It is in the final area of the OODA Loop, the act, where the Cyber Situation provides true added value. Once the commander has fully observed, oriented, and reached a decision, action can occur. The impact of this full spectrum of the OODA Loop cannot be over stated.

Prior to the full deployment of the Cyber Situation, even the best complete strategic OODA cycle will continue to take hours or days. Providing the commander with the information needed to reach the point of action meant collecting the right data, putting it in the hands of the right analyst, and providing that information to the commander. This is a cumbersome process at best, often overcome by events before the information was forwarded to the right decision maker. Since there was a time-consuming structure in place, information was unavoidably dated (even the freshest information is minutes old) and often incomplete. Thus, even under the most terrific circumstances, the commander was making a decision and perhaps employing forces without the best information.

Not only was the information incomplete, decision makers often contemplated as to whether the information their subordinates provided was reliable and credible. With the capability provided by the Cyber Situation, the information accuracy will be reliable and credible. Further, decision makers will have unobstructed access to information. In short, a decision can finally be made *with a complete picture of the battle space.*

Once a decision had been reached, the commander transmits execution orders. These orders must be properly formatted and transmitted to subordinate units for action. Again, there is an unavoidable time

lag between when the orders are transmitted and when they are acted upon. In these precious hours, the situation the commander desires to effect can change dramatically.

With the capability provided by the Cyber Situation, the commander can employ forces instantly and flexibly. Whether the weapon of choice is a laser, UAV, or F-22, through the Cyber Situation the commander has instant access to it.

What is even more compelling about the capability available through the Cyber Situation is that with the exception of the brain chip, the technologies required to field it are well along in development in 1996. Communications architectures are growing in both commercial and military applications and computer power is still on an exponential growth rate. Software, too, is becoming more intelligent. Indeed, the required capability is on the horizon.

In the end, the development of the Cyber Situation becomes a matter of priorities and trade-offs. The question that must be asked at the highest levels in the Department of Defense is whether or not bits are as important as bullets and how the DOD budget dollar must be spent to satisfy the operational requirements for air power in 2025. If what is required is the capability to provide the commander with all the information and tools to act on a decision, then the Cyber Situation is the solution.

# Appendix

## List of Acronyms and Abbreviations

| | |
|---|---|
| ARPA | Advanced Research Project Agency |
| ACC | Air Combat Command |
| AOR | area of responsibility |
| CRT | cathode ray tube |
| CJCS | chairman, joint chiefs of staff |
| CSAF | chief of staff, US Air Force |
| $C^4I$ | command, control, communications, computers, and intelligence |
| CINC | commander in chief |
| SOUTHCOM | commander in chief, Southern Command |
| CONUS | continental United States |
| DNA | deoxyribonucleic acid |
| DOD | Department of Defense |
| DSB | direct satellite broadcast |
| EEG | electroencephalograph |
| EMP | electromagnetic pulse |
| GII | Global Information Infrastructure |
| HCI | human computer interaction |
| IU | image understanding |
| IIC | Information Integration Center |
| I3 | intelligent integration of information |
| JTF | joint task forces |
| MII | Military Information Infrastructure |
| MLS | multilevel security |
| NCA | National Command Authority |
| NII | National Information Infrastructure |
| NMCC | National Military Command Center |
| NWV | New World Vistas |
| OODA | observe, orient, decide, and act |
| PDA | planning and decision aids |
| R&D | research and development |
| RMA | revolution in military affairs |
| TAV | transatomospheric vehicle |
| UAV | uninhabited aerial vehicles |
| UCAV | uninhabited combat aerospace vehicles |
| URAV | uninhabited reconnaissance aerospace vehicles |

## Bibliography

Advanced Projects Research Agency. *Intelligent Systems.* On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/ Intel_Thrust.html.

Advanced Projects Research Agency. *The SISTO Solution: Intelligent Software Systems.* On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/Overview/Solution.hmtl.

AFM 1-1. *Basic Aerospace Doctrine of the United States Air Force.* 2 vols., March 1992.

***2025*** Concept, No. 200169. ***2025*** Concept Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 900272, "Very High Altitude Balloon-Borne Systems." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 900280, "Fly on the Wall." No. 900434, "Airborne Sound Sensors." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 900438, "Ultraendurance High-Altitude Ocean Loitering Uninhabited Reconnaissance Vehicle." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 900517, "JSTARS Replacement." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 900552, "On-demand Tactical Recce Satellite Constellation." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025,*** 1996.

***2025*** Concept, No. 900604, "UAV Constellations." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 900702, "Implanted Tactical Information Display." ***2025*** Concepts Database Maxwell AFB, Ala.: Air War College/***2025***, 1996.

*Air Force Executive Guidance* (draft), HQ USAF/XOXS, December 1995.

Amato, Ivan. "Animating the Material World." *Science* 225 (17 January 1996).

Anonymous assessor comment on ***2025*** Concept, No 900702. ***2025*** Concept Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

Anonymous assessor comment on ***2025*** Paper Review Maxwell AFB, Ala.: Air War College/***2025***, 1996.

Army Space Institute. "Space Support in Mid-Intensity Conflict." In *Theater Air Campaign Studies Course Book.* Vol. 8. Maxwell AFB, Ala.: Air University Press, 1995.

Baird, Lt Col Henry, et al. "Spacelift." ***2025*** White Paper. Air University, Maxwell AFB, Ala., April 1996.

Barnett, Jeffery R. *Future War: An Assessment of Aerospace Campaigns in 2010.* Maxwell AFB, Ala.: Air University Press, 1996.

Bass, Thomas A. "Gene Genie." *Wired,* August 1995.

Carmichael, Lt Col Bruce, et al. "STRIKESTAR 2025." ***2025*** White Paper. Air University, Maxwell AFB, Ala., April 1996.

Chan, Vincent W. S. "All-Optical Networks." *Scientific American* 273, no. 3 (September 1995).

Clinton, William J. *A National Security Strategy of Engagement and Enlargement.* Washington, D. C.: The White House, February 1996.

Doughty, Robert Allan. *The Breaking Point: Sedan and the Fall of France, 1940.* Hamden, Conn.: Archon Books, 1990.

Electronics Visualization Laboratory, University of Chicago at Illinois (No date). *The CAVE: A Virtual Reality Theater.* On-line, internet, no date, available on http://www.ncsa. uiuc.deu/EVL/docs/html/CAVE.html.

Engelbrecht, Col Joseph A. ***2025*** Research director and Professor of Conflict and Change, Air War College. Maxwell AFB, Ala. Personal interview by Maj YuLin Whitehead, 17 April 1996.

Firschein, Oscar, and Thomas Strat. *Image Understanding Program.* On-line, internet, 23 July 1995, available on http://www.arpa.mil/sisto/Overview/ Image.html.

Fitzsimonds, James R., and Jan M. Van Tol. "Revolutions in Military Affairs." *Joint Forces Quarterly*, no. 4 (Spring 1994).

Fogleman, Gen Ronald R., lecture to ***2025*** participants. Air University, Maxwell AFB, Ala., 13 February 1996.

Fukuyama, Francis. RAND, Washington D. C. Electronic mail. Subject: Dross and Gold, 27 December 1995. Used by permission of author.

Garvey, Dr Tom. *Planning and Decision Aids Program.* On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/PDA.html.

Grier, Peter. "New World Vistas." *Air Force Magazine* 79, no. 3 (March 1993).

Gunning, David. *Intelligent Integration of Information (I3).* On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/I3.html.

Institute for National Strategic Studies. *Strategic Assessment 1995: US Security Challenges in Transition.* Washington, D. C.: National Defense University Press, November 1994.

Jefts, Maj Barbara, et al. "Virtual Integrated Planning and Execution Resources System: The High Ground of 2025." ***2025*** White Paper, Air University, Maxwell AFB, Ala., April 1996.

Joint Warfighting Center, Doctrine Division. *War-fighting Vision 2010: A Framework For Change.* Langley AFB, Va.: 1 August 1995.

Kalmanek, Charles, and K. G. Ramakrishnan. "On-line Routing for Virtual Private Networks." (Paper presented at the Third International Telecommunications Symposium, September 1995). On-line, internet, September 1995, available from http://www.research.att.com/hgs/infocom95/program.html.

Kolarov, Aleksandar, and Joseph Hui. "Least Cost Routing in Multiple-Service Networks: Part II." (Paper presented at the Third International Telecommunications Symposium, September 1995). On-line, internet, September 1995, available from http://www.research.att.com/hgs/infocom95/program.html.

Krepinevich, Andrew F., Jr. "The Military-Technical Revolution: A Preliminary Assessment." In *War Theory Course Book.* Vol. 3. Maxwell AFB, Ala.: Air University Press, September 1995.

Libicki, Martin C. *The Mesh and the Net: Speculation on Armed Conflict in a Time of Free Silicon.* Washington, D. C.: National Defense University Press, 1994.

McGinnis, Lt Col Michael L., and Maj George F. Stone III. "Decision Support Technology." *Military Review* 74, no. 11 (November 1994).

McKitrick, Jeffrey, et al. "The Revolution in Military Affairs." In *Air War College Studies in National Security: Battlefield of the Future.* No. 3. Maxwell AFB, Ala.: Air University Press, September 1995.

McMillan, Lt Col James. Air Force Liaison to National Security Agency. Telephone interview by Maj Scott Bethel, 26 February 1996.

Moscarelli, Paul. "Operational Analysis: An Overview." In *Strategic Structures Course Book*. Vol. 2. Maxwell AFB, Ala.: Air University Press, 1995.

Muolo, Maj Michael J. *Space Handbook: An Analyst's Guide*. Maxwell AFB: Air University Press, 1993.

Negroponte, Nicholas. *Being Digital*. New York: Vintage Books, 1995.

Norman, Maj Cindy, et al. "Man in the Chair." ***2025*** White Paper, Air University, Maxwell AFB, Ala., April 1996.

Patterson, David A. "Microprocessors in 2020." *Scientific American* 273, no. 3 (September 1995).

Petroski, Henry. *To Engineer Is Human*. Chicago: University of Chicago Press, 1989.

Psaltis, Demetri, and Fai Mok, "Holographic Memories." *Scientific American* 273, no. 5 (November 1995).

Robinson, Clarence A. "Molecular Biology Computation Captures International Research." *Signal* 50, no. 6 (February 1996).

Rogers, Craig A. "Intelligent Materials." *Scientific American* 273, no. 3 (September 1995).

Sawyer, Ralph D. *The Seven Military Classics of Ancient China*. Boulder, Colo.: Westview Press, 1993.

Scientific Advisory Board members, Comments from ***2025*** Concept Briefings Maxwell AFB, Ala., 5 February 1996.

Sears, Allen, and Robert Neches. *Human Computer Interaction Program*. On-line, internet, 23 July 1995, available from http://www.arpa.mil/sisto/HCI.html.

Sherman, Bill. *NCSA Virtual Reality Lab & CAVE*. On-line, internet, 18 February 1996, available from http://www.ncsa.uiuc.edu/VR/VR/html.

Simon, Herbert A. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. 3d ed. New York: The Free Press, 1976.

Simonsen, Maj Philip, et al. "SPACENET: ON-ORBIT SUPPORT IN ***2025***." ***2025*** White Paper. Air University, Maxwell AFB, Ala., April 1996.

SPACECAST 2020. "Leveraging the Infospace: Surveillance and Reconnaissance in 2020," SPACECAST 2020. Vol. 1. Maxwell AFB, Ala.: Air University Press, June 1994.

Szafranski, Col Richard, and Col Joseph A. Engelbrecht, Jr. "The Structure of the Revolution: Demystifying the RMA." Unpublished paper, March 1996.

Takano, Makoto, and Katsumi Fujita. "Multilevel Network Management by Means of System Identification" (Paper presented at the Third International Telecommunications Symposium, September 1995). On-line, internet, September 1995 , available from http://www.research.att.com/hgs/ infocom95/program.html.

Thomas, Peter. "Thought Control." *New Scientist* 149, no. 2020 (9 March 1996).

Tiernan, Maj Mike, et al. "In-Time Information Integration System." ***2025*** White Paper. Air University, Maxwell AFB, Ala., April 1996.

Toffler, Alvin, and Heidi Toffler. *War and Anti War*. New York: Warner Books, 1993.

USAF Scientific Advisory Board. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Human Systems and Biotechnology Volume. 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Information Applications Volume. 15 December 1995.

______. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Information Technology Volume. 15 December 1995.

______. "New World Vistas: Air and Space Power for the 21st Century," Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

Vincent, 1st Lt Gary A. "In the Loop: Superiority in Command and Control." In *Operational Structures Course Book*. Vol. 5. Maxwell AFB, Ala.: Air University Press, November 1995.

Westenhoff, Charles M., ed. *Military Air Power*. Maxwell AFB, Ala.: Air University Press, 1990.

Widnall, Dr Sheila E., and Gen Ronald R. Fogelman. *Air Force Executive Guidance*. Washington, D.C., December 1995.

______. *Cornerstones of Information Warfare*. Washington, D.C., 1995.

Zysman, George I. "Wireless Networks." *Scientific American* 273, no. 3 (September 1995).

# Information Attack: Information Warfare in 2025

Prof George J. Stein

## Executive Summary

*Information attack* is defined by the USAF as either "directly corrupting adversary information without changing visibly the physical entity in which it resides" or "activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides."

This essay argues that the proper understanding and future development of information attack, based on USAF information warfare (IW) competencies and systems, is the key to information dominance. It is likewise argued that a central obstacle to a future IW capability is that the words and definitions currently used among the Joint Staff and the armed forces to guide future development in IW are unclear, confused, and often contradictory as they fail to distinguish IW from command and control warfare ($C^2W$) and fail completely to incorporate USAF views on information attack.

The future potential in IW to substitute precise and discriminate credible information—whether by the methods of $C^2W$ (deception, PSYOP, or other means) or information attack—to a precise and discriminate target decision maker is the essence of decisive maneuver as it may position the adversary in space and time, by his own decision, in a fatally disadvantageous strategic situation. Information attack is not so much perception management as orientation management. Information is both the target and the weapon: the weapon effect is predictable error.

In future operating environments marked by ambiguity, speed, and precision effect, it will be the relative or differential advantage in information, information processing, and communication and information security that will provide the narrow margin for victory. Future USAF mastery of information attack, through airpower and space power unconstrained by artificial notions of battlefield-only command and control warfare, will provide the capability for asymmetric strategic response based on decisive and differential information advantage.

# Chapter 1

# Introduction

The strategic problems faced by the United States in the five 2025 alternate futures and the strategic problem faced in the intermediate world of 2015 identified in the ***2025*** study are identical. The strategic problem faced by the armed forces in any of these futures is the same. "The true aim," as B. H. Liddell Hart observed, "is not so much to seek battle as to seek a strategic situation so advantageous so that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this."[1] The question is whether information warfare (IW) and information attack can create this strategic situation in 2025 or even as early as 2015.

For the purposes of this essay, and for reasons which will hopefully become clear as the argument is developed, *information warfare* is defined as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities thorough command and control warfare and information attack."

Information warfare is normally understood, following the Joint Publication (Pub) 3-13, *Joint Doctrine for Command and Control Warfare* ($C^2W$) definition, as "actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while defending our own information and information systems."[2]

Information warfare is currently defined by the USAF as "any action within the information environment taken to deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations, while protecting friendly forces against similar actions."[3] For the USAF, then, bombing an enemy telephone exchange with iron bombs or corrupting the adversary's telephone switching system through electronic warfare or a computer attack are all, equally, information warfare. It is the targets, not the method of combat, which define information warfare for the USAF.

*Command and control warfare* is defined, following Joint Pub 3-13, as "a war fighting application of IW in military operations [that] employs various techniques and technologies to attack or protect a specific target set—command and control."[4]

Joint Pub 3-13 further defines $C^2W$ as the "integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary $C^2$ capabilities while protecting friendly $C^2$ capabilities against such actions."[5]

For the USAF, $C^2W$ is simply "the effort to disrupt and destroy an adversary's command and control."[6]

*Information attack* is defined by the USAF as either "directly corrupting adversary information without changing visibly the physical entity in which it resides."[7] or "activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides."[8]

## Thesis

The thesis of this essay is that the proper understanding and future development of information attack within the context of the USAF core competency of Information Dominance is the key to information warfare in the future.[9] It is likewise argued that a central obstacle to a

future information warfare capability is that the words and definitions currently used among the Joint Staff and the armed forces to guide future development in IW are unclear, confused, and often contradictory.

The USAF strategy for information warfare should be well advanced by 2015 and fulfilled by 2025 through its incorporation within the central USAF mission of the employment of air and space power. Air and space power will, as today, be conceived as global awareness, global reach, and global power. Information warfare, especially information attack, will be employed as an expression of global power made possible through global awareness and global reach. It will provide an essential component of the global presence through which national security objectives will be met and will meet the national military strategy of deterrence, promoting stability, thwarting aggression, and containing conflict, and, ultimately, projecting power to fight and win.

The key strategic issue will remain "not so much to seek battle as to seek a strategic situation so advantageous so that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this." Information warfare, especially information attack, will provide the differential advantage, especially through air and space power, to permit the United States to develop and employ asymmetric modes of operation at what are called currently the strategic, operational, and tactical levels of conflict. Asymmetric and differential strategy is the key to breaking the platform-to-platform thinking (tank-countertank, ship-antiship, etc.) that continues to dominate long-range strategic thinking inherited from the successful experience in industrial-age warfare. Information warfare is the key to asymmetric and differential strategy and, in the context of this essay, information attack as new forms of air and space power are the key to information warfare.

## The Future Environment

The development of asymmetric and differential strategy is required by the change in the range of potential military operations facing the armed forces in the emerging international security environment and the constraints consequent of both downsizing and the ever-increasing costs of traditional platforms.[10] While there may not be a settled consensus on the precise outlines of the emerging security environment, virtually all studies recognize that an unusually high plurality of diverse and untraditional tasks will challenge America's armed forces. The contemporary security environment is viewed as a generic regional contingency (or two nearly simultaneous major regional contingencies such as North Korea and Iraq), a generic niche competitor such as transnational criminal syndicates or ideological terrorists, or a generic, and yet to emerge, peer competitor.[11] The security environment can be seen as the ***2025*** study's five alternate futures "Gulliver's Travails," "Zaibatsu," "Digital Cacophony," "King Khan," and "Halfs and Half-Naughts" and the 2015 "Crossroads" intermediate future. The security environment can be described more expansively as a range of high or low end global competitors, high or low end regional competitors,[12] counterinsurgency, peace or humanitarian operations, dangerous industrial activities, weapons of mass destruction proliferation, collapsing or disintegrating states, and nonstate terrorism.[13]

The point is not that the armed forces will have to address all these challenges but that, despite downsizing and increasing platform costs, the military could be required to address any of these challenges. Absent the sudden emergence of a genuine competitor seen by the United States as having the capability to threaten American vital national security interests on a global basis, the armed forces, quite simply, must be able to do more with less or, perhaps as argued in this essay, must be able to do more by doing it differently. Information

warfare through airpower and space power may provide the capability for asymmetric response through the differential advantage of information attack in most future security challenges.[14]

In the emerging information age and the operational environments postulated in almost all the alternate futures surveyed, military operations will reflect the characteristics of the larger societies.[15] As most armed forces and many military operations become increasingly dependent on information,[16] military winners will, like economic winners in the information-based economies, need to have that core competency identified by the USAF as *information dominance* whereby the United States has "greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure" than any adversary has about the United States.[17] *Information independence* and *information security*, whereby American military power projection and even mobilization are not vulnerably dependent on the global information infrastructure, will likewise emerge as central national security issues.[18] Any discussion of information warfare, including information attack, must be understood to include equal or greater attention to defense.

The goal of information dominance, note well, is greater understanding, not total understanding. As in the emerging information economies—sometimes called winner take all economies—"victory" is often based on a very small margin or differential of talent, information, performance, or luck. It is the relative performance in those markets or activities in which having or being second-best is inadequate, even at lower cost, which brings disproportionate rewards.[19] The Olympic gold medalist who is only two seconds faster than her silver second gets the running shoe endorsement contract. The F-16 pilot who locks on only two seconds faster gets the kill. By 2025, or surely by 2050, only will be nanoseconds.

Another novel characteristic of differential performance in information-based activities is the ability to duplicate and distribute the output of the differential activity more widely, more rapidly and at relatively lower cost. Once a recording company suspects it has a platinum compact disc among its releases, millions of additional copies can be quickly manufactured, distributed, advertised, and sold planetwide.[20] Once one component of the distributed reconnaissance and surveillance satellite system locks on the target, the coordinates are duplicated and distributed by an information and communications meta-system to its customers planetwide.

The ability to conduct information-age warfare through the relatively better use of information-in-war and the ability to duplicate and distribute information warfare itself through information attack may provide the relative or differential "strategic situation so advantageous" of which Liddell Hart spoke that Sun Tzu's pinnacle of excellence could be achieved wherein the enemy is subdued by asymmetric response without battle.

Information warfare, information-age warfare, information-in-war, information, and information attack are intimately related, but they are not identical. Clarification is needed and some consensus must be reached without, however, prematurely establishing authoritative doctrine that could prevent the creative developments required to realize the future potential of information warfare. The Joint Staff was correct when it noted in Joint Pub 3-13 that the use of the term warfare in information warfare "should not be construed as limiting IW to a military conflict, declared or otherwise."[21]

**Notes**

1. B. H. Liddell Hart, *Strategy* (London: Faber and Faber Ltd., 1967), 325.
2. Joint Pub 3-13, "Joint Doctrine for Command and Control Warfare ($C^2W$)" (draft), 1995, I-4.
3. USAF, "Air Force Doctrine Document-5" (first draft), November 1995, 20.
4. Joint Pub 3–13, v.
5. Ibid., I-4

6. USAF, "Air Force Doctrine Document-5," 18.

7. USAF, *Cornerstones of Information Warfare*, 6.

8. USAF, "Air Force Doctrine Document-5," 19.

9. Gen Ronald R. Fogleman, USAF, chief of staff, and Sheila E. Widnall, secretary of the Air Force, Air Force Executive Guidance (1996), 4.

10. Theresa Hitches, "Lawmakers Call '97 Clinton Plan Unrealistic," *Defense News*, 11–17 March 1996, 14.

11. Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala.: Air University Press, 1996).

12. Jason Glashow, "Regional Powers May Gain Clout," *Defense News*, 11–17 March 1996, 36.

13. Board of Directors, USAF Long Range Planning, "Future Operating Environments," Briefing Slides, 29 February 1996, R33.

14. Joseph S. Nye and William A. Owens, "America's Information Edge," *Foreign Affairs*, March/April 1996, 20–54.

15. Pat Cooper, "Information Whizzes to Advise DoD on Future Wars," *Defense News*, 26 February–3 March 1996, 14.

16. Len Zuga, "EW Competition to Surge," *Defense News*, 19–25 February 1996, 20.

17. USAF, Air Force Doctrine Document-1, "Air Force Basic Doctrine" (draft), 15 August 1995, 10.

18. Pat Cooper, "IW Study May Guide U.S. Policy," *Defense News*, 25–31 March 1996, 39.

19. Steven Pearlstein, "The Winners Are Taking All," *Washington Post National Weekly Edition* 13 (11–17 December 1995): 6–10.

20. Gary Hamel and C. K. Prahalad, *Competing for the Future* (Boston, Mass.: Harvard Business School Press, 1994).

21. Joint Pub 3-13, I-4.

# Chapter 2

## New Ideas—New Words

The basic problem with understanding information warfare today is that there is no clear sense of just *what* is being discussed. The futurists Alvin and Heidi Toffler have argued in their recent book *War and Anti-War* that the United States armed forces need to develop a systematic, capstone concept of military "knowledge strategy" which would include clear doctrine and policy for how the armed forces will acquire, process, distribute, project, and protect knowledge and information to serve national strategy.[1] The Tofflers and others have argued that the concept of information warfare includes those information-based operations which attempt to influence the "emotions, motives, objective reasoning, and ultimately the behavior" of others.[2] The strategists John Arquilla and David Ronfeldt, on the other hand, have argued in their important essay "Cyberwar Is Coming!" that "netwar" and "cyberwar" are the key concepts for understanding information war.[3]

Originally emerging in the science fiction community as, for example, in the very thought-provoking future war suggested in Bruce Sterling's *Islands in the Net*,[4] the concepts of netwar and cyberwar provide one thoughtful starting point for exploring the military and civil/military issues of information war. Netwar, according to Arquilla and Ronfeldt, is a "societal-level ideational conflict waged in part through internetted modes of communication." That is, they suggest that what is today seen as *strategic-level*, traditional, state-to-state conflict through the use of a nation's electronic intelligence and communications assets is the essence of netwar. Unlike traditional propaganda that seeks to provide information (whether true or false) which the adversary must understand, netwar or *strategic* level information war attacks another society's epistemology and decision-making process. Netwar attacks how the adversary knows, not just what the adversary knows.

Cyberwar is seen as the *operational* level of information warfare whereby the armed forces use netwar principles, techniques, and technologies to attack the epistemology and decision-making process of the enemy armed forces—especially its commanders. Most current discussion of information war in the armed forces seems to focus almost exclusively on the tools and techniques of cyberwar rather than strategic-level netwar. At the operational level of war, a national information war or netwar strategy would be translated by the armed forces into cyberwar or command and control warfare, often referred to in military shorthand as $C^2W$. Cyberwar, in the hands of the local military commander, attacks the mind of the enemy commander through various tools, many of which are from the universe of electronic warfare, to produce bad decisions and prevent, delay, or deny information for good or militarily effective decisions.

For the purposes of this essay, information warfare is seen as analogous to netwar and, as noted above, from within the USAF view, as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy these adversary information-based activities thorough command and control warfare and information attack."

Command and control warfare would be understood by the armed forces as analogous to cyberwar. Information attack, recall, is "*directly corrupting adversary information without changing visibly the*

*physical entity in which it resides*" and is the key to both netwar and cyberwar.

Within the general and authoritative military context, however, there is little agreement on definitions or the scope of the debate. Words have meaning as, at least, the components of military doctrine and, as such, affect how each service will "organize, train, and equip" its forces to support national security policies. Much of this essay may seem to be mere semantic nit-picking, but the "right" words and definitions are vital because of the authoritative nature of doctrine. The services fight over words.[5] Whether each service will be able to make informed decisions on the future evolution of the armed forces depends on their having a coherent understanding of the promise and perils of information warfare and, especially, information attack.

As the service most likely to be able to develop its current information warfare assets embedded in global awareness and reach, and its information attack potential in global power, the USAF has a special and historic responsibility to lead clear thinking and doctrinal development for the new forms of strategic operations permitted by information warfare and information attack.

**Notes**

1. Alvin and Heidi Toffler, *War and Antiwar: Survival at the Dawn of the 21st Century* (Boston: Little, Brown & Co., 1993),141.

2. Joint Chiefs of Staff Memorandum of Policy 30, *Command and Control Warfare*, March 1993, A-4.

3. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April–June 1993): 141–65.

4. Bruce Sterling, *Islands in the Net* (New York: Ace, 1988).

5. The continuous argument over the "authority" of the joint force air component commander (JFACC) to "control" ground-support missions is illustrative. To the outsider the debate seems "theological." To troops on the ground, it's a question of life or death.

## Chapter 3

# Confused Visions

A key problem within military discussions of information warfare is that the Department of Defense, the Joint Staff, and each individual service recognize that if IW is, indeed, a new form of warfare or represents a potential for a true "revolution in military affairs," then there are important implications for the traditional roles and missions of each individual service. If, for example, "to be seen is to be killed" and hostile unmanned aerial vehicles (UAV) provide battlefield overview for smart artillery shells, armored units whose own air and space forces have not yet "blinded" the enemy will be sitting ducks. This, likewise, has implications for future access to increasingly scarce defense appropriations. If, for example, Congress becomes convinced that investing in swarms of cheap-tank-locating UAV for US Army helicopters to use to kill enemy tanks is a better idea, then this raises the obvious question "Why are we still buying tanks?" Indeed, Congress might ask whether the Joint Strike Fighter (JSF) is the better investment for plinking tanks in open terrain than an uninhabited combat air vehicle (UCAV). The military is, understandably, institutionally conservative and, as in the early discussions of airpower or current discussions of space power, more likely to attempt to fit the new into the already known.[1] Even the USAF has a legacy of platform-focused thinking.[2]

On the other hand, information warfare is the hot topic of the age and everyone wants to the part of the "Third Wave," the armed forces being no exception. Unfortunately, far too much discussion in the armed forces of IW confuses the traditional importance of information-in-warfare with information warfare or information attack itself. All those papers and briefings that begin "Information has always been central to warfare. . ." and then go on to explain that "our new computer system will get information to the warfighter" so he can "achieve information dominance on the battlefield" and thus demonstrate our service's mastery of IW, confuse information-in-war with information warfare. Whether we are digitizing the cockpit or digitizing the battlefield, this is not IW.[3] Information-in-war is absolutely vital and will be an increasingly important issue as the use of information is central to modern warfare and, more importantly, may be the sine qua non or necessary-but-not-sufficient condition for the conduct of any future traditional warfare and certainly any future information warfare. A review of the current debate within the armed forces will illustrate the problem. Ultimately, a particular USAF idea will point to the solution.

### The Joint Staff

While the current draft definition is unclassified, the official definition of *information warfare* remains classified top secret. The public, nonclassified and formal military discussion of information warfare began with the Joint Chiefs of Staff *Memorandum of Policy* (MOP)-30 (1993), "Command and Control Warfare." This document set the initial terms of debate and, consequently, most formal debate since. Most importantly, $C^2W$ was defined as "the military strategy that implements Information Warfare on the battlefield" and its objective was to "decapitate the enemy's command structure from its body of forces."[4] The legacy of Desert Storm's airpower and electronic warfare against Iraq was seen as the essence of information warfare.[5] What is really being discussed in the desert war context is, in fact, the new and creative use of information-in-war

noted by Soviet and other observers.[6] Note also that the discussion of IW starts as a battlefield topic with the result that much of the continuing debate places IW in the combat support role rather than as a new form of combat proper.

More recently, the Joint Staff has expanded the idea of information warfare in Joint Pub 3-13 (1995), "Joint Doctrine for Command and Control Warfare." Information warfare is defined, as noted above, as actions "taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending friendly information systems."[7] Here, a central and vital issue is noted. While the armed forces may attempt to gain superiority by affecting adversary information and information systems, they can defend only friendly systems. That is, the Joint Staff seems to assert that the armed forces have no military mission or authority, currently, to defend friendly information. The armed forces, it appears to be claimed, can protect military information systems only; they cannot use military assets to defend the nonmilitary information systems of the United States from adversary attempts to gain military advantage. The political debates about the restrictions placed on conveying pornography on the Internet contained in the Communications Decency Act accompanying the recently enacted Telecommunications Act are a mere skirmish compared to the civil libertarian firestorm that would result if the military claimed a role in nongovernmental information or information systems protection.[8] On the other hand, the mission of the armed forces is to defend the United States, and if hostile information attack threatens the national security, it is difficult to see why the skills and experience that the armed forces are developing to protect military systems should not be loaned to an interagency Information Security Task Force.

The Joint Staff's Joint Pub 3-13 then modifies the earlier definition on $C^2W$ first used in MOP-30 in an important but ultimately inadequate way. $C^2W$ is now seen as "a [not *the*] war fighting application of IW in military operations [not just on the *battlefield*] and employs various techniques and technologies to attack or protect command and control [not just *decapitate*]". Joint Pub 3-13 goes on to define $C^2W$ as the "integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence." That is, the integrated use of perfectly traditional information-in-war tools and techniques.

## New Thinking?

The Joint Staff, whose views on doctrine are assumed to be directive for the individual services and whose definitions thereby amplify the importance of words, is currently developing a series of ideas for war fighting in the near-future: *Joint Vision 2010-America's Military: Shaping the Future.* While not focused primarily on information warfare, *Joint Vision 2010*'s ideas are of direct relevance to the future evolution and role of IW. *Joint Vision 2010* begins with a projection of current technological trends assumed to shape the future war-fighting environment. These include: (1) the increasing precision of weapons and their means of delivery, (2) the increasing menu of weapons' effects from traditional lethality to nonlethal technologies, (3) increased stealth for both offensive platforms and invisibility of friendly forces, and (4) improvements in information systems integration, from sensors to shooters, which may permit a "dominant battlespace awareness" to include the ability to "see, prioritize, assign, and assess."[9]

These four trends, which are assumed to provide a magnitude improvement in lethality, will require *information supremacy.* Information supremacy is defined here as the "capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[10] This is,

of course, both a worthy goal and a perfect definition of information-in-war. Information supremacy, according to *Joint Vision 2010*, will require both offensive and defensive information warfare. Offensive IW will degrade or exploit an adversary's collection and use of information and will be conducted by traditional and "nontraditional" means such as "electronic intrusion" into an information and control network to "convince, confuse, or deceive enemy military decision makers."[11] Defensive IW will protect dominant battlespace awareness and provide improved command and control of friendly forces and will be conducted by traditional means such as physical security and encryption and untraditional means such as antivirus protection and secure data transmission.

*Joint Vision 2010*, then, continues the pattern of seeing information warfare as an advanced version of $C^2W$, new techniques of traditional electronic warfare (EW), and a sense that computer viruses, as a form of EW, might be important. Information supremacy is still defined, operationally, as information-in-war rather than information warfare as a potentially new form of warfare for the future. This most current Joint Staff thinking appears to have forgotten its earlier idea in Joint Pub 3-13 that the use of the term warfare in information warfare "should not be construed as limiting IW to a military conflict, declared or otherwise."

Based on the technologies of this information supremacy providing dominant battlespace awareness, *Joint Vision 2010* proposes that new concepts of operation will need to be developed. These new operational concepts (how the joint force commander will fight the fight with land, sea, air, and space forces assigned) are (1) dominant maneuver, (2) precision engagement, (3) full-dimension protection, and (4) focused logistics. These four new operational concepts will provide "Full Spectrum Dominance" to achieve massed effects in warfare from dispersed forces across the spectrum of military actions from peacetime engagement through deterrence and conflict prevention to fight and win warfare.

The key problem with Full Spectrum Dominance is not only that its notion of information warfare is still too focused on information-in-warfare but that the application of massed effects in warfare from dispersed forces still appears to assume that massing forces is the strategic problem. The Joint Staff appears to assume, naturally enough, that land, sea, air, and space forces are the only, or certainly major, means for the joint force commander to accomplish the mission. That militarily-relevant, strategic, operational, or tactical effects might be produced by information attack without combining the various joint forces in theater may be the key difference between information-in-warfare and information warfare. A brief survey of the four new operational concepts will illustrate the problem.

## Dominant Maneuver

Dominant maneuver is an operational concept that grows from the experience of the Gulf War and the evolution of US Army thinking from "Air-Land Battle" to "Force XXI Operations."[12] In essence, instead of warfare being conducted as a series or sequence of battles leading ultimately to the enemy collapse, dominant maneuver proposes to bring together widely dispersed joint forces to attack the enemy throughout the height, breadth, and depth of the battlespace by attacking all levels of the enemy's centers of gravity simultaneously.[13] Clearly, the increasing precision of weapons and their means of delivery, the increasing menu of weapons' effects from traditional lethality to nonlethal technologies, the increased stealth for both offensive platforms and invisibility of friendly forces, and the improvements in information systems integration are the technologies that permit dominant maneuver. *Joint Vision 2010* recognizes that these new weapons will "allow us to conduct attacks concurrently that formerly required massed

assets in a sequential methodology."[14] And, while these new weapons and technologies may permit us to "accomplish the effects of mass—the necessary concentration of combat power at the decisive time and place—without physically massing forces," dominant maneuver still appears to seek to "attain with decisive speed and tempo a *physical* presence that compels an adversary to either react from a position of disadvantage or quit" (emphasis added). *Joint Vision 2010* is confused. Do mass effects require physical presence by joint forces assembled from widely dispersed locations or not? And why does *Joint Vision 2010* assume that mass effects are superior to differential effects? Information warfare, advanced $C^2W$, and information attack may not need to share this assumption.

## Precision Engagement, Full-Dimension Protection, and Focused Logistics

Precision engagement and full-dimension protection make the same assumption. Precision engagement depends on a system of systems[15] that permits our forces to locate the target, provide responsive command and control, have the desired effect, assess the effect, and reengage if required. That is, we can shape the battlespace and conduct a dominant maneuver. Full-dimension protection, built on information supremacy (actually, supremacy of information-in-war), will provide multidimensional awareness and assessment, as well as identification of all forces within the battlespace. Defensive information warfare will be required to protect our information systems and processes.

Focused logistics, the final new operational concept, again illustrates the thinking that the ability to project power with the most capable forces is the central problem. The ability to fuse information, logistics, and transportation technologies; provide rapid crisis response; track and shift assets even while en route; and deliver the logistics and sustainment to the level of operations" assumes that getting stuff there for the forces is the essence of projecting power. Yes, in many cases, especially against traditional adversary's armed forces or other military operations like peace enforcement and humanitarian relief, this may be true.

Dominant maneuver, precision engagement, and full-dimension protection are clearly operational concepts that will permit the US armed forces to attain full spectrum dominance in a traditional campaign against a traditional adversary. There will be undoubtedly Saddam-revenant adversaries even in 2025. Creative USAF thinking about information warfare, however, requires that a series of unusual questions be asked: What is the future battlespace. What are forces in future conflicts? What is "there" in a future battlespace? What if the adversary is not employing forces?

*Joint Vision 2010* introduces a generally thoughtful and potentially useful set of ideas for the evolution of operational concepts for US joint forces to employ in traditional military operations across a large spectrum of conflict. It correctly recognizes information-in-warfare as one of the most important and critical aspects of near-future (c. 2010) military operations. Information superiority is, in fact, the necessary condition for future joint warfare and, as such, the Joint Staff is correct in calling for far greater attention to the promise and peril of the new technologies for the collection, processing, and secure dissemination of information-in-war. *Joint Vision 2010* is much less successful in addressing the implication for the US armed forces, and especially the USAF, if the potential for information warfare were to be something beyond a technology-based, more sophisticated version of command and control warfare.

It is, of course, the individual armed services that are tasked to organize, train and equip for the future. How are the individual armed services thinking about information warfare on the road to 2025?

## The US Army

For the US Army, "information operations" replaces information warfare as the capstone concept. Information operations are continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations.[16]

Information operations include "interacting with the global information environment and, as required, exploiting or degrading an adversary's information and decision systems." That is, the Army recognizes that information affects operations far beyond the traditional battlefield and, thus, information operations is seen as the proper "word" to include both information warfare and command and control warfare. This is a potentially important evolution in Army thinking but, currently, it results in a limited view of information warfare. Information operations may, in fact, be a better word than information warfare, and could be adopted by the Joint Staff and the other services, but only if the concept is expanded to mean more than "military operations within the military information environment."

Information warfare, for the US Army, entails actions taken to preserve the integrity of one's own information system from exploitation, corruption, or destruction while at the same time exploiting, corrupting, or destroying an adversary's information system and in the process achieving an information advantage in the application of force.[17] That is, information warfare remains in the universe of traditional platform-versus-platform thinking like "only armor can confront armor" with the information system as the new platform. Information warfare thus has been constrained to the universe of the combat support elements where techno-wizards will provide advantage for Willie and Joe to apply force with real weapons like tanks and artillery.

The US Army appears to confuse information-in-war with information warfare. The Army's goal to "assimilate thousands of bits of information to visualize the battlefield, assess the situation, and direct military action appropriate to the situation" is the use of information-in-war for traditional battle. The Army's "Information Age" *Force XXI* will "know the precise location of their own forces, while denying that kind of information to their foes" because, for the Army, information is "an essential dynamic enabling dominant military power at the strategic, operational, and tactical levels." This will be achieved by "using and protecting information infrastructures" while influencing or denying a potential adversary's use of these infrastructures.[18]

By constraining its doctrinal thinking to the infrastructure aspects of information and adopting uncritically the Joint Staff definition of $C^2W$, the US Army may have let its traditional, and proper, land-warfare focus prematurely narrow its vision to the battlespace of armor, artillery, and infantry divisions. While it is undoubtedly important that the Army study and apply its notion of information warfare to command and control warfare, it is also undoubtedly obvious that the Army must develop its concept of information operations beyond "the military information environment." information operations, if conceived synergistically with the USAF concept of information attack, are much more than "integrated support to battle command" in traditional military operations.[19]

## The US Navy

The US Navy essentially shares the same view of information warfare as does the Air Force but, like the US Army, views information operations as a means through which to conduct traditional battle. Like the Air Force, the Navy views $C^2W$ as distinct and subordinate to information warfare proper. Like the Army, the Navy appears to view IW primarily as a means to prepare for battle. The former chief of naval operations, Adm J. M. Boorda, observed recently that because of the Navy's traditional forward deployment,

"Information Warfare will give us the ability to slow and influence the enemy's decision making cycle, to prepare the battlespace before the start of hostilities, and to dictate the battle on our terms."[20] While naval doctrine for IW is in at least as much flux as that of the other services, current doctrine straddles the big view of IW and the little view of IW as $C^2W$. Operations Naval Instruction (OPNAVIST) 3430.26 defines IW as action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information *infrastructure* through exploitation, denial, and influence, while protecting friendly information *systems* [emphasis added].[21]

Platform-to-platform battle is again the model. Likewise, $C^2W$ is the "action taken by the military commander to realize the practical effects of IW on the battlefield." As a service, the Navy may be expected to develop the tools and techniques of $C^2W$ for power projection from the sea with the growing awareness of the potential for IW to project the effect of combat power far inland from the combat forces that are the source of that power.[22] The Navy recognizes that information warfare "encompasses political, economic, physical, and military infrastructures" and "expands the spectrum of warfare from competition to conflict."[23] There is an obvious potential for mutual synergy in developing asymmetric strategies between the Navy's sea and air assets and the US Air Force's air and space assets for both $C^2W$ based information warfare and information attack.

## The US Air Force

The US Air Force begins its reflections on information warfare from within its views on air and space power. For the USAF, air and space power are a means to an end, not the end itself. Like the Navy's "from the sea," airpower and space power are "done" in and from a "place" that is "more than a place": the air and space. Thus, air and space power include the projection of military force from air and space. The goal is air and space superiority as the necessary, but not sufficient, condition for the application or employment of all other military power. And, as air and space surround the globe, the USAF sees itself as having a global mission of air and space superiority, global mobility, and the precision employment of air and space assets. The same vision informs USAF thinking on information warfare.

For the USAF, currently, information is seen as analogous to air and space. Information is seen as a realm in which dominance will be contested and in which and from which military power can be employed. Like airpower and space power, information dominance is a necessary, but not sufficient, condition for the application or employment of all other military power and, likewise, is a global mission. Mastering information warfare, then, will become a USAF core competency like air and space superiority. Unfortunately, USAF thinking currently suffers some of the same internal contradictions as does the IW thinking of the Army and Navy and, more importantly, that of the Joint Staff. The issue is, again, confusion among information-in-war, information, and information warfare.

The USAF recognizes correctly that information dominance is a broad concept and describes it, in Air Force Doctrine Document 1 (AFDD-1), *Air Force Basic Doctrine*, in the war-fighting context as that condition in which the commanders have "greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure" than the enemy has about our side.[24] That is, information dominance provides a decisive degree of information-in-war that is essential for the successful application, enhancement, or employment of air and space power or, indeed, any other kind of military power. On the other hand, in AFDD-5, *Information Warfare*, information dominance is defined as that "degree of superiority in information functions that permit friendly forces to

operate at a given time and place without prohibitive interference from opposing forces."[25] As will be discussed presently, information "functions" is a problematic limitation. While information dominance must become a core USAF competency by 2025, it is only one key step, potentially, toward full-information warfare competency. Like the US Army, USAF thinking on information warfare must not be constrained to "information functions."

Unlike Joint Pub 3-13 (1995), *Joint Doctrine for Command and Control Warfare*, USAF thinking on information warfare appears to see aerospace power as not constrained by political considerations from protecting the military forces against hostile enemy information actions. That is, for the USAF, IW is any action to "deny, exploit, corrupt, or destroy an adversary's information, information systems, and information operations" while protecting "friendly forces from similar actions."[26] While the Joint Staff, the Army, and Navy see part of IW as protecting our military *systems* and military information *infrastructure*, the USAF appears to envision part of IW as defending the armed forces against enemy information actions as well as defending the military information infrastructure. The USAF is right: waiting for an electronic Pearl Harbor and then beginning the slow buildup and deployment of Army land power to apply force is not the way to prepare the armed forces for the fight, or to deter fighting, in the information age.

## Confusion

It must be admitted that current USAF thinking is confused in the area of information warfare and has not yet reached a coherence in the words that will define and guide doctrine. The USAF doctrine community, unfortunately dispersed among the Air Staff, the Air Force Doctrine Center at Langley AFB, the College of Doctrine, Research and Education at Air University, and the Air Command and Staff College and Air War College, must aim to harmonize its thinking. USAF long-range planning cannot incorporate the information warfare insights developed in research like *New World Vistas* or ***2025*** without a coherent vocabulary. Words matter.

## Air Force Doctrine Document-1, Air Force Doctrine Document-5, and *Cornerstones*

Currently, AFDD-1, *Air Force Basic Doctrine*, and AFDD-5, *Information Warfare*, postulate six roles for air and space power: control, strike, mobility, information, sustainment, and preparation. The information role is defined to include command, control, communications, and computers ($C^4$); intelligence, surveillance, reconnaissance, navigation and positioning; and the weather service. Clearly, information is seen like sustainment and preparation as combat support or combat service support to the war-fighting missions of strike, control, and mobility. According to AFDD-1, USAF core competencies, as in *Air Force Executive Guidance*, include air superiority, space superiority, global mobility, precision employment, and information dominance. As noted above, for AFDD-1, information dominance is that condition that gives greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the enemy has about our side. The core competency of information dominance, then, appears to be accomplished by the information role of airpower and space power.

In an attempt to provide the doctrinal foundation[27] for information warfare, the USAF chief of staff, Gen Ronald R. Fogleman, and the secretary of the Air Force, Sheila E. Widnall, issued *Cornerstones of Information Warfare* in 1995. *Cornerstones* proposes that the roles and missions of air and space power are not the six of AFDD-1 but four: aerospace control, force application, force enhancement, and force support. Information warfare is not a separate role or

mission but is incorporated as a component of aerospace power. In aerospace control, IW is counterinformation—actions dedicated to controlling the information realm. $C^2W$ appears under the mission of "force application." Information operations, really any action involving information-in-war, is part of "force enhancement" while the role of information in "force support" is merely noted.[28]

$C^2W$ is central to all military discussions of IW and *Cornerstones* views $C^2W$ part of the force application mission. Here the USAF has made its most distinctive and promising addition to IW thinking. *Cornerstones* modifies the model of $C^2W$ proposed by the Joint Staff and adopted by the Army and Navy from the "integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence" to "psychological operations, military deception, security measures, electronic warfare, physical destruction, and information attack."[29]

Information attack, is defined in *Cornerstones* as "directly corrupting information without visibly changing the physical entity within which it resides."[30] The USAF is the first to recognize that IW is about information itself and not just information-in-war. IW is about ideas and epistemology, what is known and how it is known, and would be waged largely, but not entirely, through adversary information systems and infrastructures. The target of war is ultimately the human mind of the adversary decision makers and, in the information age, it is information itself that is, increasingly, the center of gravity of an adversary's military, political, social, and economic infrastructure. In reality, what *Cornerstones* is asserting is that information is not just a realm in which dominance will be contested, but rather, the realm is information. Information is both the target and the weapon.

The USAF has a better sense of command and control warfare than either Joint Pub 3-13 or the Army documents. $C^2W$ is seen by the USAF as a force application mission like interdiction or close air support and it would conduct $C^2W$ through electronic warfare, psychological operations, military deception, physical attack, and security measures.[31] *Cornerstones* adds information attack to $C^2W$. As a force application mission, $C^2W$ attack (especially information attack) can be used for strategic, operational, or tactical effect. Like strategic air and space power, $C^2W$ is not just a battlefield support mission. $C^2W$ for the USAF and the Navy is only a particular form of IW, and to restrain the Navy or the USAF to $C^2W$ as the extent of its contribution to IW operations would be a foolish waste of sea, air and space power assets and capabilities. The problem comes, however, with *Cornerstones'* foundation idea of information attack doctrine in the authoritative context of official USAF doctrine represented in AFDD-1.

## The Problem

While AFDD-1 recognizes that information warfare could be used for neutralizing an adversary's will and capacity to make war, its view of information attack illustrates the same unimaginative platform-to-platform thinking as "only aircraft can contest aircraft for air superiority." That is, information attack is seen in AFDD-1 as the use of "computers and communications to directly attack the adversary's information *operations*."[32] At first glance, and given the Army understanding of information operations, this appears to move beyond attacking platforms. The problem is that an information operation is any activity that involves information *functions* and, most importantly, *Cornerstones* has defined information functions as the *technology-dependent* elements involved in the acquisition, transmission, storage, or transformation of information seen as data and instructions.[33]

Because AFDD-1, *Basic Doctrine,* defines information as "the organized network of information functions that enhance employment of forces," and *Cornerstones*

has defined information functions as the *technology-dependent* elements of the network, there is a danger that the very sophisticated idea of information attack may be seen as little different from the Army's notion of "using and protecting information infrastructures while influencing or denying a potential adversary's use" of these infrastructures. It is still a counter-platform model.

AFDD-5, *Information Warfare*, on the other hand, has defined information attack as "activities taken to manipulate or destroy an adversary's information without visibly changing the physical entity within which it resides" and information functions as any activity involving the acquisition, transmission, or storage or information.[34] The key question is, Does the USAF recognize "any activity" beyond attacking (and defending) the technology-dependent information infrastructure as part of information attack?

Authoritative USAF thinking has not demonstrated how IW could be used for "neutralizing an adversary's will and capacity to make war" beyond a slightly more expansive notion of command and control warfare tied to tricky computer hacking to enhance the employment of forces. The USAF must rethink AFDD-1 and AFDD-5 to realize the potential of information warfare implicit in a creative development of information attack. The USAF must also reject the idea that IW is only to enhance the employment of forces, and must break free of the mantra of jointness wherein airpower and space power are discussed only within the context of supporting the joint force commander. Air and space power will permit information attack in 2025, and information attack may be the differential that permits asymmetric strategic operations by aerospace power alone in war and peace.

**Notes**

1. Andrew F. Krepinevich, "The Pattern of Military Revolutions," *The National Interest*, no. 37 (Fall 1995): 30–42.
2. Carl H. Builder, *The Icarus Syndrome: The Role of Air Power Theory in the Evolution and Fate of the U.S. Air Force* (New Brunswick, N.J.: Transaction Publishers, 1994).
3. James M. Dublik and Gordon R. Sullivan, *Land Warfare in the 21st Century* (Carlisle Barracks, Pa.: US Army War College Strategic Studies Institute, 1993).
4. Joint Chiefs of Staff Memorandum of Policy 30, 3.
5. Edward Mann, "Desert Storm: The First Information War?" *Airpower Journal* 8, no. 4 (Winter 1994): 4–14.
6. Mary C. FitzGerald, *The Soviet Image of Future Wars: "Through the Prism of the Persian Gulf"* (Washington, D.C.: The Hudson Institute, 1991); and V.K. Nair, *War in the Gulf: Lesson for the Third World* (New Delhi: Lancer International, 1991).
7. Joint Pub 3-13, I-4.
8. Daniel Brandt, "Infowar and Disinformation: From the Pentagon to the Net," *NameBase NewsLine*, No.11, October–December 1995, 11 available from: gopher://ursula.blythe.org/00/pub/NameBase/newsline.
9. *Joint Vision 2010–America's Military: Shaping the Future* (1995), 5.
10. Ibid., 7.
11. Ibid.
12. United States Army Training and Doctrine Command, *Force XXI Operations: TRADOC Pamphlet 525-5* (August 1994).
13. Ibid., 2–9.
14. *Joint Vision 2010*, 7.
15. William A. Owens, "The Emerging System of Systems," *Military Review* 75, no. 3 (May–June 1995): 15–19.
16. United States Army Training and Doctrine Command, *TRADOC Pamphlet 525-69: Concept for Information Operations*, August 1995, 2.
17. Ibid., 3.
18. United States Army Training and Doctrine Command, *TRADOC Pamphlet 525-69*, 2.
19. Ibid., 2.
20. Air Land Sea Application Center, *Information Warfare/Information Operations Study*, December 1995, 16.
21. Ibid., 17.
22. Navy Public Affairs Library, *Copernicus—Forward $C^4I$ for the 21st Century*, June 1995, 2.
23. Ibid., 7.
24. USAF, Air Force Doctrine Document-1, 10.
25. USAF, Air Force Doctrine Document-5 , 19.
26. USAF, Air Force Doctrine Document-1, B-3 quoting AFDD-31 (first draft).
27. USAF, *Cornerstones of Information Warfare*, 16.
28. Ibid., 11.
29. Ibid., 5.
30. Ibid., 6.
31. Norman B. Hutcherson, *Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base* (Maxwell AFB, Ala.: Air University Press, 1994).
32. USAF, Air Force Doctrine Document-1, 11.
33. USAF, *Cornerstones of Information Warfare*, 2.
34. USAF, Air Force Doctrine Document-5, 19.

# Chapter 4

# Rethinking Information Warfare

The USAF strategy for information warfare will be developed by 2025 through its incorporation within the central USAF mission of the employment of air and space power. Airpower and space power will, as today, be conceived as global awareness, global reach, and global power.

The USAF has seen correctly that information is like air and space; it is a realm in which superiority will be contested and from which power can be projected or engagement conducted. Information, for the USAF, is likewise just as much part of the physical universe as the other realms in which it operates and, indeed, may be "the" realm. Thus, information warfare will be conducted according to the same principles as are air and space operations. If this axiom is correct, and there is no scientific reason to assume that information is not grounded ultimately in matter and energy, then the characteristics of information warfare are analogous or parallel, not merely metaphorical, to the contemporary and future characteristics of airpower and space power.[1] The contemporary and future characteristics of air and space power, and the key to its centrality to those differentials which argue that aerospace power is the instrument for an asymmetric strategy are, of course, global awareness, reach, and power. Global awareness provides, increasingly, exact and timely information. Global reach permits a range and responsiveness to engage, not just fight, throughout the global battlespace. Global power, increasingly marked by the ability to apply precise and discriminating effects of power, will permit an asymmetric response which leverages the differential information-in-war advantage provided by global awareness and the information-based planning and execution control provided by global reach.

## Global Awareness

Global awareness, in the view of *New World Vistas: Air and Space Power for the 21st Century*, is that the USAF can use "affordable means to derive appropriate information about one or more places of interest after a delay which is short enough to satisfy operational needs."[2] Global awareness requires the USAF to have the ability to detect and understand friendly and adversary activities in space, on the surface, and in the air. Global awareness in 2025 will require, additionally, detection and understanding in the info-realm or cyberspace. In the info-realm, global awareness must provide the information-in-war essential for information attack on the strategic, operational, or tactical centers of gravity of an adversary's military, political, social, and economic infrastructure.[3]

Various capabilities to provide global awareness to support traditional air and space power employment will, obviously, be vital in providing for the employment of information attack in the alternate and intermediate futures of the ***2025*** study and, indeed, any future security environment. There are also info-awareness-specific capabilities that will need to be developed.

The set of required capabilities for future global awareness include a new generation of sensors based on a distributed system of satellites, surface sensors, and standoff systems based possibly on Uninhabited Combat Air Vehicles (UCAV).[4] As it may be too much to expect even the new Joint Requirements Oversight Council to force the development of a common USAF/Army/Navy system and standards of database management and data communication, an implied requirement of continued USAF leadership of the global awareness system is a generic

crosstalk capability with sister services and coalition partners.[5]

A specific set of USAF requirements for information attack, defined as directly corrupting information without visibly changing the physical entity within which it resides, can be identified within the general requirement of database management within global awareness. As in the classic North American Air Defense Command nuclear attack defensive system, the information must be detected and identified before there can be any talk of interception or destruction. Consequently, a reorientation in thinking about the traditional target sets for militarily-relevant intelligence gathering needs to occur as the information warfare battlespace is the information-dependent global system-of-systems on which most of the "strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure" increasingly depend. That is, not only must the question "What and where are the data?" on which these infrastructures depend be answered, but, equally important, "What are the structures and patterns of human activity depending on these databases and communications infrastructures?" Information attack requires more than a knowledge of wires and, consequently, suggestions for an Information Corps of techno-wizards would only produce platform thinking as hackers fought hackers.[6]

Locating and corrupting a database that is of marginal relevance to an adversary's will and capacity to make war is a waste of scarce resources. It is the relevant information differential that is central to information attack as apparently benign activities or databases can hide potentially hostile cyber-strike capabilities. Thus, while global awareness for information attack appears to be about "everything," at the pragmatic level, artificial intelligence search-architectures for differentially relevant "information" must be designed by the Air Force Intelligence Agency, the Air Force Institute of Technology, and other labs under the Air Force Material Command. The technologists, however, must be led by the strategists in the same way as planning the traditional air campaign requires a coherent knowledge of the adversary systems.[7] It is the patterns of human activity that are central.

As asymmetric response may be the best strategic choice in many cases, the relevant information target for global awareness attention may not be those data and communications systems that support directly the adversary's fielded military activities (the Joint Staff's nominal target for information warfare and the adversary systems most likely to be best defended), but those other supporting data, infrastructure, and patterns of activity on which most contemporary and future military operations depend. While specific information attack activities will be discussed below in the section on global power, one example of the "other" data systems which might be subject to discriminate or precision asymmetric information attack are an adversary's Supervisory Control and Data Activity (SCADA) systems for the operation of the air traffic control or fuel pipeline network.[8] Clearly, then, the SCADA databases and networks of potential adversaries must be detected, identified, and mapped.

At the most generic and nontechnical means level, global awareness for information attack will require monitoring commercial developments in information infrastructure architectures and capabilities, among whom these systems are employed, and how and by whom they are used. And, as it should be obvious that there is a defensive aspect of information warfare in that these capabilities will be used by an adversary against the United States or an ally, careful monitoring will be required of developments in commercial-off-the-shelf (COTS) systems which could be used to attack industrial processes (for example anti-SCADA programs), financial and communications networks, and

breakthrough systems that might provide differential advantage in information management and communications. Equally important, patterns of human activity or organizational change that suggest a developing potential for hostile information attack must become part of the normal business of global awareness. Identification of commercial industrial espionage in info-systems, even by an ally, should be presumed to indicate the intent to develop an information attack capability.

To support information attack in the near-future, whether for information warfare or $C^2W$, USAF global awareness systems will need to develop and incorporate specific database and database management and correlation acquisition to its collection, processing and analyzing of activities currently monitored for planning and execution control.[9] This set would include, logically, standard intelligence and surveillance architectures, command, control, and communications systems, especially systems designed to detect and defeat information attack, target and tracking, guidance, and navigation systems, especially space-based and other long-range communication capable systems, and attack assessment and reconstitution systems.[10] The intelligence challenge will be more demanding than when the United States faced only one strategic peer competitor.

To support future capabilities for information attack in the asymmetric engagements required in the ***2025*** study, current USAF global awareness and monitoring activities will need to be expanded to include the other database and database management information systems. These might include general computer systems such as the Internet and the World Wide Web, power generation and distribution systems, industrial, financial and transportation systems, and, in general, any system which might be used by an adversary to launch an information attack, first on US armed forces, and ultimately, on other domestic information assets.[11] Such an expansive system of monitoring will be essential to protect these domestic assets on which US joint force power projection itself ultimately depends.

It is important to note that the reorientation of intelligence activities needed to support information attack (and defense) in both the near and 2025 future as a USAF global awareness mission is in complete conformity with current US law. The object of USAF global awareness is not the American domestic database and database management systems. Domestic counter intelligence and law enforcement agencies will develop an ability to monitor adversary activities in the United States. On the other hand, USAF global awareness assets may be the main source of intelligence support for alerting law enforcement agencies charged with protecting domestic information-dependent activities from adversary information attack about hostile capabilities.[12]

## Global Reach

Global reach is usually thought of as the ability of deploy aircraft from the continental United States or out-of-theater bases into the area of interest in a rapid and timely fashion. The role of air refueling is likewise central to global reach. Whether delivering bombs, special forces troops, or humanitarian assistance, the speed, range, and lift of aircraft are usually seen as the key issues in delivering what is required. This differential ability to reach out with rapid, discriminate, and precise effect is central to the USAF's leading role in asymmetric response even in traditional operations.

A more sophisticated view recognizes that the USAF ability to deploy and fly its space-based assets anywhere, anytime is essential for contemporary reconnaissance, communication, and command and control. This capability will be even more important in 2025. Discussions of direct broadcast satellite sensor-to-shooter or satellite-to-joint-surveillance-target-attack-radar-system (JSTARS) and then to all relevant parties is a

central component of global reach. The capabilities of aircraft like *Commando Solo* or follow-on variants based on UAVs or direct broadcast satellites and the variety of on board electronic warfare wizardry already deployed on most US combat aircraft are recognized, again, as central to global reach. Future requirements for air refueling will include servicing UAVs and UCAVs used for information attack, perhaps via batteries recharged by airborne or satellite-reflected, ground-based lasers.[13]

Many of the current and projected global reach capabilities in speed, lift, and all-weather performance based on ever more precise navigation will be even more central to information warfare and information attack in 2025. As the new generation of sensors based on a distributed system of satellites, surface sensors, and standoff systems is developed, USAF "atmospheric" global-reach thinking must evolve to include the mission of precise, point-of-use delivery of surface-based sensors. Global reach must develop the capability to deliver sensors, or other information attack hardware, with the same stealth, speed and, most importantly, precision now focused primarily on bombs. Global reach requires that ultrahigh altitude air drops of information attack devices via, perhaps, Global Positioning System (GPS) based steerable parachutes must receive the same attention currently given precision guided munitions.[14]

The future role of USAF space reach is, of course, central to global awareness and global power. Specific space-based information warfare capabilities such as direct broadcast of video-morphed news broadcasts by the enemy leader announcing surrender are easy to imagine. These "Hollywood" capabilities, however, may not be the best use of space by the USAF. Whether protecting free access to space, defending against hostile use of commercial satellites by an adversary, developing an antisatellite capability, or having launch-on-demand capabilities, any and all of these could have some application to information attack (and defense). However, as the liberal, free-market, information-based economies of the United States and our allies are among those most likely to depend on "freedom of the high frontier," the USAF should be hesitant about the militarization of space. On the other hand, if information attack is correctly identified as directly corrupting information without visibly changing the physical entity within which it resides, the potential for information attack against the United States or its allies via space-based commercial or neutral third-party systems cannot be ignored.[15] As shutting down the space-based planetary navigation or communications systems may not be an option for either technical or political reasons,[16] USAF global reach to support global awareness and power will require a residual capability to provide launch-on-demand or activation-on-demand of secure systems.

## Global Power

USAF global power, increasingly characterized by the ability to engage with precise and discriminating effect, permits the asymmetric strategic response which leverages the differential information-in-war advantage provided by global awareness and the information-based planning and execution control provided by global reach. USAF global airpower and space power capabilities increasingly demonstrate that the USAF's concept of *decisive* maneuver, engagement with precise and differential or relative superiority, should replace the *Joint Vision 2010* concept of *dominant* maneuver.

Dominant maneuver, recall, proposes to bring together widely dispersed joint forces to replace the sequential march through the enemy's fielded military, population, infrastructure, and system essentials to get to the adversary leadership to convince him to change his behavior by attacking the adversary throughout the height, breadth, and depth of the battlespace and by attacking all levels of the enemy's centers of gravity simultaneously. The adversary system goes into shock and its ability to

react is paralyzed. Dominant maneuver has become the Holy Grail of joint force employment. In reality, this massive and simultaneous engagement of joint forces appears to be required primarily because the joint force campaign planners lack the real-world, near-real-time knowledge of the key structures and patterns of activity, information, communication, or databases on which the adversary is dependent. *Joint Vision 2010*'s "Full Spectrum Dominance," a very traditional American vision of war fighting, reflects the continuing inability to recognize the potential of information warfare. The emerging mission of USAF global awareness, as noted previously, must be to address this requirement to identify the strategic and militarily relevant information differential. Dominant maneuver may be an obsolete concept for the exercise of military power in many of the security challenges of the near-future. Decisive maneuver, seen by the USAF as engagement with precise and differential or relatively superior air and space power assets, will be the future strategic choice and the rational use of scarce military resources. It will be the way to do more, differently.

Information warfare in the dominant maneuver universe is likewise usually discussed analogously to cumulative war in that a full-spectrum attack on the adversary's information infrastructure results in rendering him blind, deaf, and dumb. Lacking command and control of his military forces then, his actions are supposed to become chaotic and his forces are thus easier to defeat. It has not, however, been demonstrated that a blinded, chaotic actor represents the enemy decision maker from whom one could expect rational compliance with US strategic objectives.[17] Battle is supposed to be about "some" thing, not "any" thing. Total information warfare against the adversary may be closer to "making the rubble bounce" than intelligent war fighting.

Information attack, on the other hand, as seen by the USAF more narrowly than full-scale IW, will be the essential component of decisive maneuver and may, in some situations, be the only exercise of discriminate power required to shape relatively predictable actions and produce the "strategic situation so advantageous" that US security objectives are met without dominant maneuver of the whole joint team. For the USAF to develop the capability for discriminate, precision information attack, new USAF research must address precise modeling of a potential adversary's Markov chains[18] and revisit the theories of power distribution control.[19]

## Further Refinements

Information warfare can be direct or indirect. While it may appear at first counterintuitive, indirect IW involves creating information (or disinformation) that the adversary must observe if the intended effect is to be achieved.[20] A false radio transmission that is not intercepted by the enemy is a waste of electrons. For the USAF, indirect IW as a form of perception management[21] will be executed in the future most often by the traditional means of command and control warfare: psychological operations, military deception, security measures, electronic warfare, and physical destruction.[22]

Direct information warfare involves changing an adversary's information without involving the requirement that it be observed. Direct information warfare, counterintuitively, bypasses the adversary's perceptive or observing functions.[23] Thus, direct IW will be executed in most cases by information attack: directly corrupting information without visibly changing the physical entity within which it resides.[24] The goal is to "access the adversary's base of information used for decision making, thereby minimizing the unpredictability of the perceptive process."[25] Based on the information provided via USAF global awareness capabilities and the ability to deploy provided by global atmospheric and

space reach, both indirect and direct USAF IW capabilities will be developed.

Planning for information attack would need to include the assembly of baseline critical data, the analysis of adversary essential networks or systems, and human activity patterns. Thus, as the essential first step, a vulnerability assessment of the processes, procedures, and physical characteristics of adversary information-dependent activities would need to be developed and continually updated.[26] To prepare to use information attack in asymmetric response, USAF info-warriors in 2025 must be guided by the principle that adversary military force is ultimately an output or peripheral of a weapons system and its sustaining, often civil, infrastructure.[27] Corrupt the sustaining system and, like a diver deprived of his oxygen supply, the adversary military force may be ineffective.

The chief technical requirements for information attack that would need to be developed by the USAF in 2025 would include awareness of future trapdoors in computer programs and components; future systems to defend and penetrate, in peace and war, critical military, commercial, and educational, information-dependent systems; and future systems to protect against and deploy corrupt information via common carrier globally distributed information systems, false-flag (commercial products), or third-party (coalition partners) systems.[28] Capability for precision stealthy deployment of sensors and information attack devices would need to be developed. Most importantly, alternative sets of databases and communications architectures will need to be developed and kept on the shelf in the future. Returning to the classic North American Air Defense Command model, once the pattern of information-dependent human activities is identified, the information target can be detected and identified, and the data on which the activity is dependent could be intercepted, destroyed, or corrupted by appropriate replacement. Is this science fiction? The Air Force Scientific Advisory Board notes that "methods for attacking information systems are under development"[29] and future "technologies and concepts for intelligence gathering and information attack in the commercially based, distributed global information system of 2025" can be discussed.[30]

If, for example, an emerging peer competitor of the type identified as "Khan" in the ***2025*** study were to conduct missile tests or war games in an area or manner deemed unacceptable to the US or an ally, a standard response might be to redeploy a US carrier battle group to the region to signal or deter. The asymmetric strategic response would be to conduct information warfare through several means. Data could be manufactured and broadcast from USAF satellite assets which showed to all parties listening that Khan's missiles are woefully inaccurate as second-stage burn was only 87 percent complete. This would be indirect IW. The future capability needed for direct IW through information attack would be the insertion of the identical data into Khan's own sensor systems and the sensor systems of third parties, say a regional ally of Khan, to confirm the data. Finally, and most ambitiously, Khan's sensor architecture could be corrupted so that even if true data from, say, a commercial satellite system were examined, the corrupt results would still obtain. That one or two other sources might provide the correct data only complicates further the adversary's orientation and analytic problems. The battlespace of future conflicts could be shaped by the long-term effects of nonlethal disorientation information attack.

**Notes**

1. Robert J. Wood, *Information Engineering: The Foundation of Information Warfare* (Maxwell AFB, Ala.: Air War College Research Report, 1995). Available from Air University Library, Maxwell AFB.
2. Air Force Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century - Summary Volume* (1995), 19.
3. USAF, Air Force Doctrine Document-1, 10.
4. *New World Vistas*, 22–24.

5. *Chips* 14, no.1 (January 1996). Special issue on the Defense Message System (DMS).

6. Martin C. Libicki and Jim Hazlett, "Do We Need an Information Corps?" *Joint Force Quarterly*, no. 2 (Autumn 1993): 88–97.

7. John A. Warden, *The Air Campaign: Planning for Combat* (Washington, D.C.: National Defense University Press, 1988).

8. Bruce M. DeBlois et al., *Dropping the Electric Grid: An Option for the Military Planner* (Maxwell AFB, Ala.: Air University Press, 1994).

9. *New World Vistas*, 26.

10. Michael J. Witt, "U.K. to Test Civil Computers in Secure Defense Arena," *Defense News*, 1–7 April 1996, 12.

11. Pat Cooper, "War Game Reveals IW Vulnerabilities," *Defense News*, 4–10 March 1996, 33.

12. *Legal Aspects of Information Warfare Symposium—Conference Proceedings* (Maxwell AFB, Ala.: Air Force Judge Advocate General School, November 1995).

13. Frank Oliveri, "Unmanned Aircraft May Dominate Air Warfare," *Defense News*, 4–10 March 1996, 8.

14. *New World Vistas*, 32.

15. Michael R. Mantz, *The New Sword: A Theory of Space Combat Power* (Maxwell AFB, Ala.: Air University Press, 1995).

16. Jennifer Heronema, "Pentagon Must Give Equal Time to Commercial Users of GPS," *Defense News*, 1–7 April 1996, 58.

17. George J. Stein, "Information War-Netwar-Cyberwar," in B. R. Schneider and L. E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell AFB, Ala.: Air University Press, 1995), 153–70.

18. Wood, 35–47.

19. George E. Orr, *Combat Operations $C^3I$: Fundamentals and Interactions* (Maxwell AFB, Ala.: Air University Press, 1983).

20. USAF, *Cornerstones of Information Warfare*, 4.

21. USAF, Air Force Doctrine Document-5, 7.

22. Norman B. Hutcherson, *Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base* (Maxwell AFB, Ala.: Air University Press, 1994).

23. USAF, Air Force Doctrine Document-5, 7.

24. Lawrence G. Downs, *Digital Data Warfare: Using Malicious Computer Code as a Weapon* (Maxwell AFB, Ala.: Air War College, 1995). Available from Air University Library, Maxwell AFB.

25. USAF, Air Force Doctrine Document-5, 7.

26. Pat Cooper, "U.S. Must Boost $C^4I$ Models, Simulation," *Defense News*, 1–7 April 1996, 46.

27. Frank M. Snyder, *Command and Control: The Literature and Commentaries* (Washington, D.C.: National Defense University Press, 1993).

28. Paul DiJulio et. al., "Communications-Computer Systems: Critical Centers of Gravity," in Air Command and Staff College, *Air Campaign Course 1993–Research Projects* (Maxwell AFB, Ala.: ACSC, 1994), 283–94.

29. *New World Vistas*, 42.

30. Ibid., B–15.

## Chapter 5

# Into the Future—Information Attack in 2025

Information attack, while "platform-based" in the physical universe of matter and energy, is not the only counter-platform, and the USAF must move its authoritative doctrinal thinking in AFDD-1 away from the idea that information attack involves only the use of computers and communications.[1]

Indirect information warfare attacks the "observation" level of knowledge at which the information must be perceived to be acted on. In many cases, indirect IW will be platform-to-platform as, for example, offensive and defensive electronic warfare, jamming or other interference systems, and psychological operations via the successor systems to *Commando Solo*. It may, however, rely on nonelectronic old fashioned military deception and psychological operations. Offensive and defensive indirect IW will grow in importance as information dependence creates information targets for an adversary to exploit against the United States. The armed forces could become "vulnerable sophisticates" in the worlds of 2025.[2] Counterplatform is not everything, but counterplatform attack will not be obsolete.

Direct IW as information attack, on the other hand, corrupts the "orientation" level of knowledge so that adversary analysis, whether artificial-intelligence or information-technology based or, most importantly, based in the mind of the human decision maker, decides and acts with full confidence in either the information observed or the integrity of his (machine or human) analytic processes.[3] Information attack, then, may or may not be counterplatform.

The future potential in information warfare to substitute precise and discriminate credible information—whether by the methods of $C^2W$ (deception, PSYOP, or other means) or information attack—to a precise and discriminate target decision maker is the essence of decisive maneuver as it may position the adversary in space and time, by his own decision, in that strategic situation so disadvantageous "that if it does not of itself produce the decision, its continuation by a battle is sure to achieve this." It is not so much perception management as orientation management. Information is both the target and the weapon: the weapon effect is predictable error. If, on the other hand, information attack fails and battle is necessary to convince the adversary the old-fashioned way, the differential information-in-war advantage provided by global awareness and the information-based planning and execution control provided by global reach may permit decisive maneuver by USAF air and space assets of such speed, precision, and discriminate force that the joint task force never leaves the continental United States execute its dominant maneuver.

In the future operating environments marked by ambiguity, speed, and precision effect, it will be the relative or differential advantage in information, information processing, and communication and information security that will provide the narrow margin for victory. Future USAF mastery of information attack, through air and space power unconstrained by artificial notions of battlefield-only command and control warfare, could provide those capabilities for asymmetric strategic response based on decisive and differential information advantage in most future security environments.

Information warfare, in this essay, was defined as "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities thorough command and control warfare and information attack." The only question is whether the USAF is prepared to take those actions.

**Notes**

1. USAF, Air Force Doctrine Document-5, 7.

2. Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* 9, no. 1 (Spring 1995): 56–65.

3. Wieslaw Gornicki, "W cieniu bomby L," *Przeglad Spoleczny "DZIS,"* no.11-62 (1 November 1995): 48–60 [translated by the Foreign Broadcast Information Service as "In the Shadow of the L-Bomb."] Gornicki calls IW "the absolute ultimate weapon of the White Man" and fears the CIA is slipping viruses into computer software exported to a future "enemy of freedom."

# A Contrarian View of Strategic Aerospace Warfare

Lt Col Robert D. Gaudette Maj Christopher A. Cook
Maj Terrence J. Foley

## Executive Summary

This paper presents a new vision of strategic aerospace warfare that expands and looks beyond the traditional roles and missions of strategic aerospace forces. Current joint doctrine divides warfare into three separate levels: strategic, operational, and tactical. Actions in these levels are many times planned, prepared, and executed with very different emphasis on size, scope, and importance. This division of objectives has met with varied success throughout history with many tactical victories leading to strategic defeats. It is important not to disregard the lessons of history as the theory needed to operate effectively in the year 2025 is developed.

The alternate future scenarios developed in the ***2025*** study suggest the future will involve many different interconnected actors. Even in the year 2025, much of the general population may still not have access to communication systems. However, the leadership of most of these organized entities will. Understanding the effect of knowledge transfer systems upon the global system is the key to strategic warfare in the year 2025. As knowledge transfer systems expand, all leaders in the global community will have access to near-real-time information. As a result, the boundaries between the current strategic, operational, and tactical levels of warfare will fade, resulting in only one level of war—the strategic level.

Strategic aerospace forces will be used to influence the will of the adversary's leadership. Due to the impact of information, all actions will have some measurable effect on the contextual elements that make up the leadership's decision-making process. To successfully influence and maintain harmony in the global system of 2025, our aerospace forces must

1. View the world as a single system by expanding from a regional to global perspective.
2. Recognize the strategic impact of daily operations and decisions on the global system.
3. Create a leadership corps to be expert practitioners in the art of war.
4. Reorganize for efficiency and creativity. Organizations must be flattened to maximize the interchange of knowledge and exploit the potential of a leadership corps.
5. Pass the responsibility for both war fighting and organization, training and equipping to the same location to take advantage of all actions having a strategic impact.

In the year 2025, successful application of all aerospace forces will be conducted with the intent to obtain the appropriate strategic effect while maintaining a balance of the global system. Information dominance is the key to proper employment of the functional concepts of Global Awareness, Global Reach, and Global Power. It is information that allows aerospace power to create strategic influence against an adversary's leadership. To effectively exploit this information vision, organization and capabilities must change to ensure that the strategic aerospace forces of the United States are prepared to skillfully employ the art of war and continue to support the will of our national leadership.

# Chapter 1

## An Introduction to Strategic Warfare in 2025

"Strategic Aerospace Warfare." These words convey many grand images. A misty morning with hundreds of B-17s forming up for their mission to Berlin. Perhaps a more modern image of Minuteman missiles in silos and B-52s loaded and cocked on alert. The goal of strategic aerospace warfare has historically been to destroy or render useless the "enemy's war making capacity and national will."[1] "Precision" attacks upon petroleum production, ball bearing factories, weapons production facilities, power generating and distribution networks, communications, and even the enemy population, have characterized target sets used in conducting strategic aerospace warfare. The results of these campaigns reported in *The United States Bombing Surveys*, *The Air War in Southeast Asia*, and *Gulf War Air Power Survey Summary Report* indicate that strategic attack by aerospace forces fell short of the claims made by the airpower experts.[2] In these conflicts the bomber didn't always get through to the target, and if it did, the desired effect was not always as planned. Certainly strategic aerospace warfare has been effective in meeting the requirements of some of the national objectives that brought this country to war during the last 50 years, but it has fallen short of the claims proposed by Gen Giulio Douhet, Gen Billy Mitchell, and Col John Warden.

In this paper we will examine the role of aerospace forces in conducting strategic warfare in 2025. Some have suggested not much will change in the conduct of strategic aerospace warfare between now and the year 2025.[3] They propose we plan and acquire systems that are faster and strike with greater precision. This may be a much too simple approach and one, if wrong, could leave us unprepared to succeed in the world of 2025. To be successfully fought and won, wars of 2025 need to emphasize the subtleties of strategy and influence rather than relying predominantly on the precision use of brute force. Col Richard Szafranski in his article, "Neocortical Warfare? The Acme of Skill," correctly assesses the future of warfare as going beyond the "application of physical force . . . [in the] quest for metaphysical control."[4] But he stops short of recognizing that warfare in the future will not be conducted as it is today. Warfare today is characterized by local or theater clashes with adversaries mostly isolated from the global system. The actors that comprise the world in 2025 will be more connected much as organs are connected within a larger organism. This does not say the US won't engage locally. What it does say is the successfulness of engagements in 2025 will be measured in terms of both short- and long-term effects upon the balance of the global system. Strategic aerospace forces will remain an important part of the US military as they will provide at times the only viable means to create the strategic influence required to preserve the balance of the global system.

Just as medical science has advanced in its knowledge of preventive medicine, the strategic aerospace forces of 2025 will be used to avoid and prevent conflicts. Strategic forces should be used to provide greater preventive control and influence to maintain the health of the global system. The armed forces of today are blunt and brutish and can be called upon to perform "surgery" on the small organs within the larger global organism whenever symptoms of sickness appear. This surgery is expensive both in treasure and human

lives and may not be the ideal treatment for the sickness that has befallen the organism. The strategic aerospace forces of 2025 will need to continue to learn, organize, and become better equipped to provide care to the global organism and if at all possible to prevent the violent clash that constitutes war. Carl von Clausewitz in his book *On War* states, "War never breaks out wholly unexpectedly, nor can it be spread instantaneously."[5] There are opportunities to avoid force-on-force conflict and they must be maximized in 2025. Strategic forces will be used in 2025 much as an acupuncturist uses needles to influence the body's central nervous system to maintain the balance of the human organism. Broadening our focus on high technology and systems to emphasize strategy and the art of warfare will ensure that our strategic aerospace forces are effectively employed daily to productively shape the ever-changing global system.

Our strategy and doctrine for 2025 must be sound. History is replete with actors assuming they possess either the ultimate in strategy or a weapon that provides an impenetrable shroud of invincibility. The French provide a fine example of the doctrine of static warfare becoming dogma between the world wars. The French doctrine of methodical battle, stressing firepower, was inadequate to overcome the mobile battle of blitzkrieg.[6] Assuming the next war would be like the last, France poured millions of francs into building the Maginot Line and creating a mobile reserve force to rapidly move to forward positions in Belgium while leaving the area bordering the Ardennes forest lightly defended.[7] French organization and command and control were predicated on the Germans' conducting another version of the 1914 Schlieffen Plan.[8] The French believed the Maginot Line was impenetrable and would keep invaders from the east off French soil forever. The Germans saw the Maginot Line as simply an obstacle that if avoided would be unable, unlike an army, to pursue them as they drove to and secured the Channel. Six weeks after the start of "Plan Yellow," the whole of France fell, only years after the end of World War I and the French celebration of victory over Germany.[9] This history lesson suggests that dogmatic adherence to doctrine, weapon systems, organizational structures, service obligations, or even thought processes will make our aerospace forces vulnerable to an adversary today and even more so in the year 2025.

## A Perspective

This paper presents a perspective of strategic warfare that challenges the status quo. The following chapters aim to show the differences and similarities between 1996 and 2025 that we can expect to find in the future. To understand the role of strategic aerospace in 2025 we will begin by examining the joint doctrine of 1996. With this foundation we will leap forward to 2025 and examine the world of the future that we must begin to prepare for today. This vision of 2025 will highlight the changes in personnel selection and training, organizational structures, and planning tools that may be required to effectively operate in the global system supporting United States objectives.

### Notes

1. Dr James A. Mowbray, "Air Force Doctrine Problems: 1926–Present," *Airpower Journal* 9, no. 4 (Winter 1995): 25–26.

2. The United States Strategic Bombing Survey, Summary Report (European and Pacific War), 1945; reprinted in *The United States Strategic Bombing Surveys (European War) (Pacific War)* (Maxwell AFB, Ala.: Air University Press, 1987); Herman L. Gilster, *The Air War in Southeast Asia: Case Studies of Selected Campaigns* (Maxwell AFB, Ala.: Air University Press, October 1993); and Thomas A. Keaney and Eliot A. Cohen, *Gulf War Air Power Survey Summary Report* (Washington, D.C., 1993).

3. The Strategic Aerospace Warfare Study (SAWS) panel commissioned by General Fogleman, chief of staff of the Air Force, also tackled the question of strategic warfare in 2025. Their yet unpublished paper proposes the nation-state will still be the predominant actor in

2025 and that strategic aerospace warfare will take place between nation-states.

4. Col Richard Szafranski, USAF, "Neocortical Warfare? The Acme of Skill," *Military Review*, no. 11 (November 1994): 43.

5. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 78.

6. Robert A. Doughty, *The Breaking Point* (Hamden, Conn.: Archon Books, 1990), 325.

7. Ibid., 11.

8. Ibid.

9. Doughty, 331.

## Chapter 2

# The World of 1996

Today's joint doctrine considers strategic targets to be those things that support the adversary's capability to meet his strategic security objectives. The types of things targeted today may include the adversary's infrastructure, energy production, transportation, and command and control networks. The mission of today's strategic aerospace forces is to conduct operations to influence these target sets in attaining theater objectives that support our national security strategy.

Today's joint doctrine divides war fighting into three levels of combat operations: strategic, operational, and tactical. Though clear boundaries are not delineated, the levels are based upon their contribution to achieving the specific level's objectives.[1] The levels attempt to link strategic objectives with tactical action. Figure 2-1 represents the current joint doctrine divisions of warfare.

Actions in these three levels are many times planned, prepared, and executed with very different emphasis on size, scope, and importance. This division of objectives has met with varied success throughout history with many tactical victories leading to strategic defeats.


**Figure 2-1. Current Joint Doctrine Levels of War**

Sitting Bull led the Sioux and Cheyenne Indian nations to an overwhelming tactical victory over Lt Col George Armstrong Custer at the battle of Little Big Horn. What Sitting Bull did not foresee was that the tactical action taken could magnify into a strategic defeat. Public outcry from the East demanded prompt reparation for the "massacre." The unintended result forced upon the Indians was an unexpected move to reservations in Missouri. Sitting Bull was forced to flee to Canada and lost the ability to negotiate a fair settlement to the conflict. The Sioux and Cheyenne lost their homeland.[2]

## Levels of Operation in 1996

The strategic level of aerospace warfare is conducted against those resources that have been identified as supporting the ability of the adversary to meet his strategic objectives and goals. The operational level links the tactical employment of aerospace forces with the strategic objectives. The tactical level focuses on the engagement of aerospace units in combat.[3]

Today great care is taken by planners to develop strategy from national policy. As the strategy flow from the strategic to the tactical level it increases in detail and focuses on the cause-and-effect relationships that are required to produce the desired end state in the operational area. The narrowing of focus is necessary in the current organization of the military to direct forces for employment. Theoretically, all actions down to the tactical level support the strategic theater objectives, and the strategic objectives are known and understood throughout the theater of operation. However, in practice, tactical orders such as the air tasking order (ATO) do not clearly delineate the strategic aims

supported by the tasking. A planner somewhere in a planning cell understands the causal relationship; the fighter in theater most likely does not.

Planning in 1996 uses cause-and-effect modeling to determine the desired courses of action to take in conducting an operational campaign. An example of this modeling is the Warden five-ring model.

The Warden five-ring model describes the enemy as a system.[4] The system is broken into five different categories: Leadership, System Essentials, Infrastructure, Population, and Fielded Forces. Information has been suggested as the "bolt" that holds the system together. War is conducted by precisely attacking critical nodes supporting the centers of gravity (COG) identified in the rings of the enemy system causing catastrophic effects and reducing the ability of the enemy system to operate effectively. The aim of warfare in this theory is not focused directly on the enemy's fielded forces or even the strategic intentions of the enemy leadership. Instead, Warden's five-ring approach, by creating paralysis, attacks the ability of the enemy system to effectively operate and project power. Paralysis is created by shocking the enemy system with synchronized attacks throughout the system's structure (parallel attack). The leadership is not affected directly because it is usually well protected. Success and imposition of our will on the adversary are attained by threatening the adversary's continued existence as a modern industrialized nation. With no capability remaining to reconstitute, the enemy system collapses. It is truly a form of "death by a thousand cuts."

The five-ring theory clearly demonstrates the linear cause-and-effect processes that are used today to plan engagements. Because the world is not linear, the cause-and-effect relationship will eventually break down. When this happens a disconnect will occur between the desired strategic objective and the lower-level operational and tactical objectives. To help overcome this shortfall and win the engagement conclusively, the strategic, operational, and tactical levels must be simultaneously attacked and the enemy nation effectively destroyed. This was how this nation fought in the historical conventional engagements of this century: World War I; World War II; Korea; Vietnam; and Operation Desert Storm.

Today using the three levels of warfare philosophy, the war is won by holding the continued existence of the adversary's nation at risk. Over the years this philosophy has worked with varied levels of success. It is arguable whether our most recent engagement in Desert Storm was successful. Five years and many millions of dollars after hostilities officially ceased, our presence in the region is still required and Saddam Hussein is still influencing the global community.[5] It seems our victory fell short of Warden's claim that strategic paralysis of the enemy system would lead to the changing of the enemy leadership's will.[6] It is important to not disregard the lessons of history as the theory needed to operate effectively in the year 2025 is developed.

**Notes**

1. Joint Publication (Pub) 3-0, *Doctrine for Joint Operations*, 1 February 1995, ix.

2. *Encarta 95*, 1995 ed., s.v. "Sitting Bull."

3. Joint Pub 3-0, II-3.

4. Col John A. Warden III, "Air Theory for the Twenty-first Century," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues* (Maxwell AFB, Ala.: Air University Press, September 1995), 107–8.

5. On the five-year anniversary of the end of Operation Desert Storm Saddam Hussein held a victory celebration. Though his country is a disaster and remains under an economic embargo, Saddam's influence and power is still felt in the region. Employment by Saddam of weapons of mass destruction is still a concern in the region.

6. Warden, 104.

## Chapter 3

# The Vision of Strategic Aerospace Warfare in 2025

## Alternate Futures

Alternate futures or scenarios illuminate the challenges that will be faced in the future. The alternate futures of 2025 bound the future that could actually exist. Bounding the problem is much like the quantum description of particles within an atom. We do not know exactly where the particle is at any given time, but we do know the boundaries within which it exists. Examining the boundaries and understanding the themes common in the alternate futures planning space suggests an effective means of organizing, planning, training, and equipping of forces to meet the challenges posed in the year 2025.[1]

The alternate future scenarios developed in the ***2025*** study suggest that the future will involve many different interconnected actors. The landscape of 2025 may be dominated by one, two, or many actors, and these actors may even take the form of nonstate entities. The overall system will be complex, and even the smallest actor could wield some amount of influence upon the global system. It is accepted that even in 2025 much of the general population of the world may still not have access to communication systems and decision-making processes within their entities. Even so, the leadership of most of these organized entities will. Understanding the effect of knowledge transfer systems upon the global system is the key to successful prosecution of strategic warfare in 2025.

As knowledge transfer systems (such as intelligence nets, commercial satellite imagery, Internet, global news networks) expand, all leaders in the global community of 2025 will have access to information in near real time. As a result, the boundaries between the current strategic, operational, and tactical levels of warfare will begin to fade. This continued blurring of the already indistinct divisions of the classical levels of warfare leads to a situation where eventually all military action will have a measurable strategic impact on the adversary leadership's decision-making processes. The pervasiveness of information and knowledge available to the enemy must be exploited and incorporated into the planning, preparation, and execution of all military actions to shape the strategic response of the global system.

## The 2025 Vision

In the world of 2025, strategic aerospace forces may be called upon by our national leadership to provide flexible options for influencing the global environment. The following items stand as landmarks that will challenge our nation's aerospace forces in the year 2025.

- The global game board in 2025 will be very crowded and interconnected.
- Unpredictable nonlinear response to strategic influences will be experienced because of the rapidity of multiplexed feedback within the global system.
- Understanding the feedback processes will be crucial to accurate prediction of results. Outcomes will be influenced more by the type and condition of the feedback present than the degree of complexity or the number of variables in the system.
- The nation-state will not have a monopoly on influence and power. Whether 2025 is uni-, bi-, tri-, or multipolar, influence and power promoted by even

small actors will reverberate throughout the global system.

- Information will dominate the global landscape with rapid cycle times measured against the speed of light. Much of what we see today, we will continue to see in 2025 just one million times faster.

Strategic aerospace warfare in 2025 will do much more than shape the battlefield; strategic aerospace forces will be used to shape the global system. In 2025 all things must be measured against the effect they will have on both the adversary leadership and the global system. An almost prescient application of aerospace forces will be required to ensure our desired end states are attained without upsetting the delicate balance of the global system. Good situational awareness of the global system must be maintained to prevent military action from creating undesired effects and subsequent vulnerabilities that could be exploited by an adversary.

The world of 2025 is full of strategic dangers and pitfalls. In an era of declining defense spending, aerospace systems must be acquired that will effectively influence and harmonize the global system of 2025.

## Harmony amidst Cacophony

Success in 2025 will require the United States to redefine "winning." War in 2025 will be even more difficult to fight as a zero-sum game with a clearly defined winner and loser. In 2025, successful methods to win will need to embrace as much as possible a win-win philosophy. Harmony is a concept that addresses this desire.

The many external and internal factors that may influence the global system in 2025 create a vision that could be characterized as a cacophony. Even the alternate futures dominated by a single nation-state or nonstate actor will be interconnected such that even small actors and their influence must be considered when examining the global system as a whole.

An illustration of a cacophony is a symphony orchestra before the beginning of a concert. With no direction from the conductor each instrumentalist (actor) is playing his own tune (following his own objectives). To an observer the sound generated at this point is discordant and very noisy. Upon the direction of the conductor (currently our role as the world's sole superpower) each instrumentalist provides his contribution to the piece in harmony with the other players in the orchestra. This action, under the direction of the conductor, creates a composite sound from the orchestra (global system) that is in balance. Note that the harmony and richness of sounds of the different instruments blend to create a sound that is more beautiful than if all played the exact same melody. For this reason, the output of the whole orchestra is much greater than the sum of the individual instrument parts. Unfortunately it takes only one instrumentalist (actor) playing out of tune (bucking the conductor's objective) to create discord for all the others in the system. To be effective the conductor must capture the attention of all the instrumentalists and demonstrate the mutual benefits that can be enjoyed by all as they follow the conductor's leadership. Certainly this example does not propose that the US dominate the global system to the point of removing the individual sovereignty of the various nation-states and other actors. Rather, it is suggested that effective leadership must be performed in the global system to mold an environment that is mutually beneficial for all involved.

The world of 2025 will be full of challenges as the US seeks to interface successfully in the global arena. Careful understanding of strategic effects will allow aerospace forces to be used effectively to maintain harmony in the global system. Lack of understanding of strategic effects in the application of aerospace forces could lead to disaster.

## Chaos or Nonlinear Response

How do we prevent our adversaries from responding differently from the way we desire? Chaos has been considered as a possible solution to the dilemma of predicting the response of the global system to strategic influence. Can chaos understanding be used in this situation to help us predict the unpredictable? Maj Bruce DeBlois in his paper "Deterministic Philosophical Assumptions in the Application of Chaos Theory to Social Events" shows that chaos is applicable to only deterministic systems. Chaos as a science may not be applied to a nondeterministic system. Social systems (at least those considered to be desirable) include the human element of freewill and are therefore nondeterministic.[2] This means unpredictable nonlinear response can be expected from the interconnected global system, and chaos theory will not help predict the results. Understanding the nonlinear global system's reaction to influence must be the focus of our planning and employment of strategic aerospace forces in 2025.

## Nonlinear Systems and Strategic Analysis

The decision-making process used by planners must be balanced to ensure information derived from linear modeling and simulation does not over influence the acquisition of and decision to use certain types of weapons systems. James Polk has suggested that in some cases, "We have been led astray by computerized wargames . . . because the primary determinant of victory in these exercises is a preponderance of firepower [not the subtleties of human will]."[3] The focus in determining the proper influence to apply is dependent on the contextual elements of the adversary, the predicted reaction of the adversary to the applied influence, and the predicted second-order effects on the global system. These all must be predicted as accurately as possible using nonlinear techniques including the genius of intuition.

The pinball machine is perhaps a good illustration of planning and applying appropriate and inappropriate influence on a system. In a pinball machine a steel ball is shot to the top of a ramp comprised of a matrix of bumpers, pads, rails, and other obstacles. As the ball rolls down the ramp it is influenced by Newtonian physics and the obstacles it comes into contact with. Some obstacles take energy from the ball, some add energy. The path the ball takes is the result of the influences upon it. For an element to have influence (change the path of the ball) the ball must come into contact with it. A decision path of a notional leader is shown in figure 3-1 below.

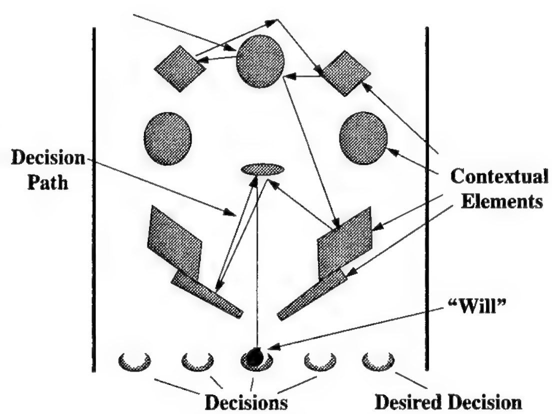



**Figure 3-1. The Pinball Machine**

The ball in this example represents the "will" of the adversary's leadership during one decision cycle. The ball contacts various obstacles that represent the various contextual elements within the adversary's system in its journey down the ramp. The will of the leadership is influenced by the contextual elements within the system. As illustrated below (fig. 3-2), the effect of the contextual elements upon the decision process can change as the priority of values changes (such as the different values displayed by leaders in war versus peace) and as external factors such as information are added and subtracted from the system.

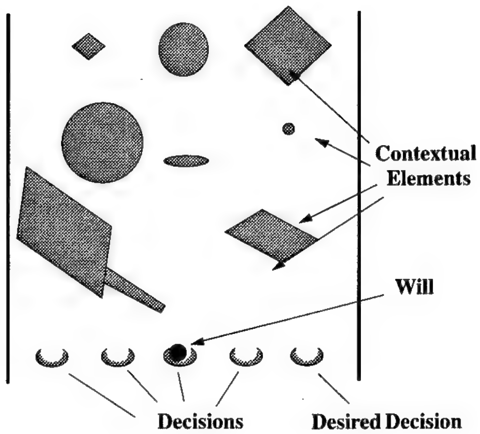



**Figure 3-2. The Pinball Machine with Influence Added**

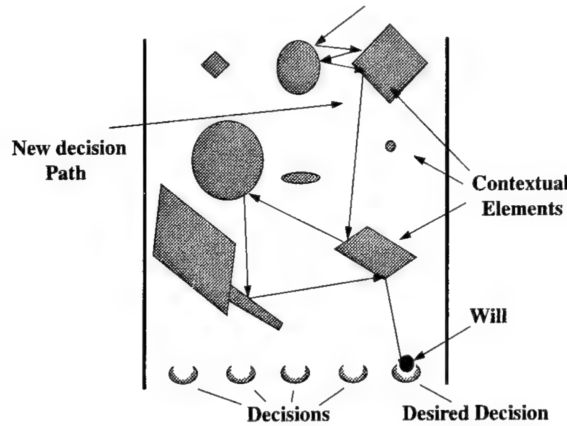



**Figure 3-3. The Pinball Machine with a New Decision Path Defined**

By understanding the contextual elements that are affecting the adversary's decision process and applying the appropriate influence (in this example by adding/ removing or perhaps changing the power exerted on the ball by an obstacle), the will of the leadership can be directed to a more desirable conclusion (as defined by our own national security policy). The inappropriate application of influence in this system would be

1. influencing contextual elements that are not considered by the enemy leadership,
2. adding or subtracting too much energy and deflecting the will away from the desired result, and
3. creating problems equal to or greater than those we are attempting to resolve through second-order effects on the global system.

As defined by Clausewitz, the focus of military action is on the will of the enemy leadership.[4] Notice in this example that there are no levels of engagement (e.g., strategic, operational, tactical). What really matters is the effect of the action on the enemy leadership's decision cycle (fig. 3-3). This suggests that in 2025 no action at any level of warfare should be undertaken without regard to its expected influence on the will of the enemy leadership.

Due to the human element, it will always be impossible to determine and predict every potential response an adversary will have resulting from a strategic influence. Preparation and training must be accomplished to maximize the understanding and correct identification of the contextual elements that may influence the will of the adversary's leadership. Correct prediction will prevent surprise and unnecessary bloodshed.

The world of 2025 will require both subtle and sometimes severe influence to direct the adversary leadership's will to harmonize with our desired endstate. To recap from the previous illustration, proper influence of the leadership's will in 2025 will require

1. that the influence used will affect the leadership's will,
2. that the influence used will properly deflect the enemy's will in the direction of our desired end state, and
3. that the use of the influence will not create any undesirable (defined by our policy) secondary effects on the rest of the global system.

War is a two-way street. Influence applied to an adversary must be done while protecting the contextual elements that will influence our own nation's leadership.

## Formlessness

We must protect our nation's vulnerabilities by using deception as Sun Tzu suggests to appear distributed and formless to any adversary.[5] On the road to 2025, technology must not drive the acquisition decision process. The temptation is great but it must be resisted to ensure that technology does not create systems that are easy targets for a motivated adversary. The development of monolithic systems and the creation of force capabilities around them makes aerospace forces vulnerable to the enemy's influence. In the year 2025, our forces must be flexible enough to influence the varied contextual elements of the adversary's leadership or they will be ineffective. Strategic aerospace forces must be capable of changing rapidly to adapt and apply influence to the changing contextual elements of the adversary.

## Single Level of Operation in 2025

In the year 2025, daily activity will require planning and prediction to assess the effects of influence on the global system. This is not to say every action in the world will have a strategic effect, but rather, every action may have an effect and an effort should be made to understand and direct the outcome. The key to the interconnection of the global system, as previously stated, will be information.

Information will create a metaphysical relationship between all the global actors. Since the leadership within the global system will have access to many varied sources of information, each military action will have the potential of affecting the contextual elements that influence the leadership's expression of will. The Cable News Network (CNN) factor has already shown its enormous power to influence. Some cases in point: During Operation Desert Storm, CNN televised a multitude of coalition attacks against Iraqi forces and other targets. It is very likely these images and the knowledge that the whole world was seeing them influenced Saddam. The CNN images certainly seemed to influence our own leadership. President Bush's decision to end the ground campaign after 100 hours was driven by the desire to prevent unnecessary slaughter and images of the unbelievable destruction on the "road of death" leading from Kuwait back to Baghdad from appearing on CNN and affecting the solidarity of the coalition. This decision allowed the Republican Guard to escape to the north (maybe in retrospect the wrong thing to let happen), but it kept the coalition together (at the time maybe a greater concern). In a more recent example, there were no forces in Somalia that could have stood against the US forces deployed there in 1994. The images on television of a dead US Army Ranger being dragged through the streets created a large public outcry in the US. Two weeks later the US withdrew from Somalia. This result probably exceeded all expectations of the Somali warlords who directed that incident. It is a good example of the effect that information has today on the leadership's will and the fusing of the levels of warfare into one. In other words, a strategic goal resulted from a tactical action. It may be helpful to view the effect of information upon any event in 2025 as shown below.

Event + Effective Application of Information = Appropriate Strategic Effect

or maybe even

Event × Effective Application of Information = Appropriate Strategic Effect

In any case information is a factor that must be considered and used in the application of military power to create strategic effects and influence the will of the adversary's leadership.

## The *2025* View of Warfare

In the year 2025 successful application of all aerospace forces (since every aircraft, satellite, acquisition decision, etc., might have a strategic influence depending on the

adversary) will be conducted with the intent of obtaining the appropriate strategic effect while maintaining the balance of the global system. Information Dominance is the key to proper employment of the 1996 aerospace functional concepts of Global Awareness, Global Reach, and Global Power. As illustrated in figure 3-4, it is information in 2025 that will allow aerospace power to create strategic influences that affect the adversary leadership. Further explanation and development of the functional concepts of Global Awareness, Power, and Reach are contained in appendix A.

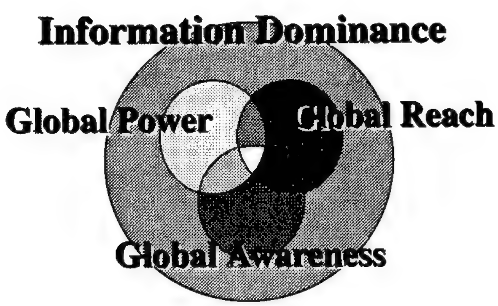



**Figure 3-4. The *2025* View of Warfare**

Successful operation in 2025 requires understanding and acceptance that even the most mundane items may have great strategic impact. Even today information magnifies small actions into large effects, such as the criminal actions of a few sailors and Marines in Okinawa, which threaten the continued basing of US troops on the island.[6] The subtleties of influence will define the world of 2025. Effective exploitation of information will allow aerospace forces to meet the challenges of the future.

**Notes**

1. Alternate futures were developed by the ***2025*** study team using creative thinking techniques. The alternate futures that were developed describe the extremes that could exist in the year 2025. Further information on the 2025 alternate futures can be found in the yet unpublished white paper, *Alternate Futures for 2025.*
2. Maj Bruce M. DeBlois, "Deterministic Philosophical Assumptions in the Application of Chaos Theory to Social Events" (Unpublished paper, School of Advanced Airpower Studies, Maxwell AFB, Ala.).
3. Quoted in Chet Richards, *Modeling and Analysis or Strategy and Decision?* (Marietta, Ga.: Lockheed Corporation and the Georgia Institute of Technology, 1991), 1.
4. Clausewitz, 75.
5. Sun Tzu, *The Art of War,* trans. by Samuel B. Griffith (London: Oxford University Press, 1963), 66–67.
6. "U.S. will give back some Okinawa land," *The Montgomery Advertiser,* 15 April 1996, 4A.

## Chapter 4

# The Strategic Decision Maker in 2025

In the year 2025 our forces will operate in an environment much different from today. All operations (training, exercises, deployments, force application) will insert power into the global system, causing shifts in the balance of power and a resulting system response. Daily aerospace activities will be used to maintain or upset the balance of the global system and project power to guide decision-making processes. Idealistically, proper application of power will create true harmony within the global system. Realistically, strategic influence will be required daily to fix yesterday's problems, while creating tomorrow's problems. This chapter addresses three areas, that if concentrated on today, may in the next few years provide a strategic force more capable of successful influence in 2025. The areas of focus proposed are training, organization, and planning.

## Training for Strategic Understanding

As previously discussed, the global system will be characterized as nonlinear but not chaotic due to its nondeterminant nature. To effectively operate in the world of 2025 all aerospace force leaders' training must increasingly emphasize the art of war. The focus on the "soft" ideas of persuasion, agility, subtlety, and influence as found in Sun Tzu and "fog and friction" espoused by Clausewitz will help personnel understand and influence nonlinear systems. Training with simulation as done today is very cost-effective, but in simulation it is extremely difficult to insert the human element or moral factors described above.[1] Mathematical limits are imposed on computers by Godel's theorem and the Church-Turning thesis that will prevent a simulation from ever being able to completely replicate the human mind.[2] War will always remain an art. The focus on high-technology weapon systems must not be allowed to cloud the creative critical thinking of aerospace personnel to make accurate and sound strategic decisions on the application of strategic influence.

The environment of 2025 will require a special kind of officer, planner, and leader who can view and understand the global system and manipulate influence to direct the will of the various actors that make up the system. Just as pilot training selects individuals with certain demonstrated qualities to fly fighters instead of transports (or vice versa), individuals who have the ability to think and make correct strategic decisions in a nonlinear environment must be selected to monitor and influence the global system.

This idea of a notional planner/strategic decision maker leads to the creation of a leadership corps. Much like the Prussian General Staff, individuals with demonstrated potential early in their career (two to four years) should enter specialized training to increase their abilities to judge and influence nonlinear systems in preparation to become members of the planning staff. By the time these individuals reach the 15- to 20-year point they should be experts in the operational art of warfare. The key characteristics of the leadership corps should be the ability to quickly synthesize information and the ability to rapidly choose a course of action that correctly influences nonlinear systems without upsetting the balance of the larger system. The individuals comprising the leadership corps should be trained to measure, understand, and guide the global system using the appropriate application of the military instrument of

power (in conjunction with the other instruments of power) to maintain harmony. Those who are unable to effectively operate in this complex environment should be moved out of the leadership corps.

## Organizing for 2025

In the year 2025 the organizational structure used by aerospace forces must be optimized to both plan and direct proper influence upon our adversary's leadership. The proposed highlights of this future organization are

1. innovation and awareness that allow seamless planning and simultaneous execution within the theater and subregion of operations,
2. adaptability and flexibility to transform the organization to effectively meet the posed challenges,
3. nearly instantaneous feedback after influence is applied to understand the adversary's new or continued strategic intent, and
4. a distributed and dispersed network to create invulnerability.

The function of any organization is to maximize the capabilities of the individuals who are assigned to it. The organization created for 2025 must maximize the leadership corps's ability to direct global influence. Effectiveness in the year 2025 will be somewhat proportional (due to the nonlinearity of the system) to our ability to dominate the information spectrum. According to Alvin and Heidi Toffler, "A revolution is occurring that places knowledge, in various forms, at the core of military power. In both production and destruction, knowledge reduces the requirements for other inputs."[3] The function of the 2025 military organization will be the management and application of knowledge. Knowledge is different from information in that it has been processed. Inf received, understood, and has been provided a measure of significance to be used by the rest of the organization.

To effectively manage knowledge, organizations must be as flat as possible, and staffed with creative thinkers. Combining the staffs that organize, train, and equip with the war-fighting staffs would maximize efficiency in properly assigning influence since the decision to conduct or not conduct an exercise next to an adversary's country might be more effective in directing the will of the adversary leadership than dropping a bomb. Remember, everything in the year 2025 can have a measured influence on the global system if it has an effect on the will of our adversaries. So it doesn't make sense as we prepare for 2025 to continue to separate these functions. The same staff that creates and measures strategic influence must also organize, train, and equip. Some ideas and proposed changes to today's organizational structure that will prepare the Air Force to meet 2025 are contained in appendix B.

Knowledge must be easily shared internally and externally to the organization. Some type of low-level artificial intelligence may help route knowledge throughout the organization to the proper decision makers without excessive time delays or human intervention. This will enable the sharing of knowledge without time lost interpreting or translating. With knowledge available and decision makers properly trained, the planning staff of 2025 is now ready to plan.

## Planning in 2025

"Strategic" targets in the year 2025 are a function of the contextual elements that influence the decision-making capability of the adversary's leadership. They may or may not correlate to the western standard ideas of petroleum, oil, and lubricants (POL) distribution and storage areas; electric power; $C^3$; and so forth. It is entirely dependent on who and what makes up the adversary's leadership decision-making process—what influences the will. To clearly understand the appropriate influences to undertake, we must know what makes our adversary tick. What does he hold to be

ground truth? What does he hold close? How does he perceive the United States? How does he regard world opinion? Where is he vulnerable? The answers to these questions will result in a strategic plan. Combining the strategic vulnerabilities of each global actor with our own vulnerabilities and capabilities will provide a vision of the global system. With this vision and understanding we can more effectively influence the global system to maintain harmony. This task is enormous. To properly accomplish it we must create organizations and tools to support our leadership corps's decision-making process.

As noted by Sun Tzu, success is more likely attained when we know both our enemy and ourselves.[4] By thorough examination of both the contextual and operational elements in each region and effective measurement of the effects of previous influences applied, we may be able to more accurately model the boundaries of the nonlinear global system.

So where should strategic aerospace warfare be planned? Is this purely a national command authorities (NCA) or a Department of Defense (DOD) function? Is it a function of Intelligence? Where exactly should strategic analysis be accomplished? This question has been haunting aerospace planners since the inception of airpower. Lt Col Donald Wilson, while serving as director of the Air Strategy and Tactics department of the Air Corps Tactical School (ACTS) in 1939, directed that students be informed of the necessity to carry intelligence work far enough to provide a detailed analysis of objectives and targets within those objectives. Maj Muir S. Fairchild, who taught the national economic structure course, took a different view by stating that gathering complete information concerning targets was "a study for the economist, statistician (or) technical expert, rather than the soldier."[5] For more than 50 years we have been depending on experts outside the DOD to determine what we should influence. This has been ineffective in providing information to the war fighter in a timely manner to properly apply strategic influence. The leadership corps, as experts in the operational art, must be able to effectively measure and control the influence upon the global system.

But who is going to perform the functions of this strategic analysis? This function should be performed at the theater level, with interaction to a national-level agency that would provide a global view. To properly understand and truly create knowledge from the tremendous amount of information that is available in the year 2025 we propose the creation of a strategic decision support system.

## Strategic Decision Support System

To achieve a time-limited response capability and reduce our decision cycle time, a planning and measurement system must be designed to effectively analyze and support the leadership corps's decision process. In the year 2025 the use of societal models must be used to understand and predict the consequences of our day-to-day military operations, as well as our crisis response.

A streamlined decision-making process should emphasize knowledge flow. The leadership corps must be able to rapidly identify capabilities and requirements necessary to deal with any situation that may arise and direct the proper influence to be applied. This type of decision support system will be required to effectively reduce our observe-orient-decide-act (OODA) loop[6] and provide a framework for appropriate decisions.

As influence is applied, the leadership corps must be able to effectively monitor and assess the global strategic impacts of the influence. There must be a feedback into the strategic decision support system framework that allows timely review of the impacts and creation of new decisions based on the new knowledge.

Again the concepts of Godel and Church-Turning demonstrate that "human understanding can not be an algorithmic activity."[7] Machines will never have the intelligence to replace the human mind. But, machines do provide effective analytical tools to support decision making. Albert Clarkson in his book, *Toward Effective Strategic Analysis*, argues that computer systems are important analytical tools because they don't forget history and are free from operator bias.[8] How often has history been repeated? Proper design and application of a strategic planning system will result in successful application of aerospace power in the year 2025.

**Notes**

1. Chet Richards, *Modeling and Analysis of Strategy and Decision?* (Marietta, Ga: Lockheed Corporation and the Georgia Institute of Technology, 1991), 11.

2. Rodger Penrose, *Shadows of the Mind* (New York: Oxford University Press, 1994), 51.

3. Alvin and Heidi Toffler, *War and Anti War: Making Sense of Today's Global Chaos* (New York: Warner Books, Inc.), 80.

4. Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith (London: Oxford University Press, 1963), 84.

5. Lt Col Thomas A. Fabyanic, *Strategic Air Attack in the USAF*, Research report no. 5899 (Maxwell AFB, Ala.: Air University Press, April 1976), 41.

6. Maj David S. Fadok, *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis* (Maxwell AFB, Ala.: Air University Press, February 1995), 16. OODA stands for Observe, Orient, Decide, and Act and has been developed by John Boyd to explain the process that is necessary to effectively engage and defeat an opponent. If you can operate your OODA loop faster and more accurately than your opponent can operate his, you will gain a decisive advantage that will lead your opponent to confusion and defeat.

7. Rodger Penrose, *Shadows*, 51.

8. Albert Clarkson, *Toward Effective Strategic Analysis* (Boulder, Colo.: Westview Press, 1981).

## Chapter 5

# Conclusions and Recommendations

The world of 2025 will be complicated and challenging. Knowledge transfer networks will interconnect the global system causing it to react much like a single, large organism. Strategic aerospace forces can be used preventively to influence and maintain the balance and harmony of the global system.

The year 2025 will have only one level of warfare—the strategic level. Strategic aerospace forces will be used to influence the will of the adversary's leadership. All action will have some measurable effect due to the impact of information on the contextual elements that make up the leadership's decision-making process.

Now is the time to begin to prepare for the future of 2025. To successfully influence and maintain harmony in the global system of 2025 our aerospace forces must

1. Recognize the world as a single system. The vision and decision-making processes used by strategic aerospace forces must be expanded from a regional to a global understanding.
2. Recognize the strategic impact that our day-to-day operations and decision making have on the global system. Daily decisions must be measured and gauged by their influence on the global system.
3. Create a leadership corps to be the expert practitioners in the art of war.
4. Reorganize for efficiency and creativity. Organizational structures must be flattened to maximize the interchange of knowledge and the potential of the leadership corps.
5. Pass the decision responsibility for both war fighting and organizing, training, and equipping to the same location. This will take advantage of all action having a measurable influence on the global system.

The year 2025 will present the United States with many challenges. Strategic influence will come in many forms and varieties. The knowledge organizations will be necessary to function successfully in the future global system and must be created now. Vision, organization, and capabilities must change to ensure that the strategic aerospace forces of the United States are prepared to skillfully employ the art of war and continue to support the will of our national leadership.

# Appendix A

## Global Awareness

The futures of 2025 dictate a requirement for the United States to maintain information dominance. As the Internet and other means of communication make the world a smaller place, the need for near-real-time information processing (awareness) will be critical. With the global game board becoming more crowded and interconnected, the US must have the awareness to deal with all the variables that will make up the strategic level of war. Global Awareness is the ability to predict and measure the impact of aerospace forces on the global system.

The United States must be able to quickly assess situations and determine the appropriate response to each situation to meet our strategic objectives. To accurately assess a situation and determine the appropriate response, we must create officers trained in the subtleties of strategy and warfare. To help the decision-making process, technology must be employed to produce a system that supports the strategic decision-making process. This system must help planners accurately predict in a timely manner, by applying proper significance to the barrage of information overloading our systems, the strategic effects of any regional decision. By properly balancing the planners of 2025 with their tools, awareness and understanding of the global system can be created. That understanding will be used to reach and touch our adversary's decision processes.

### Global Reach

Global Reach in the year 2025 is the ability of the US to influence an adversary leadership's contextual elements anywhere, at anytime. Aerospace forces are unique in that they have agility, speed, and range that allow continental US basing and still retains timely response to influence the adversary. Strategic implications of Global Reach include the ability to deny an adversary sanctuary, or the ability to cause disruption within an adversary's system by interjecting "force" into that system. To deny sanctuary, or to cause disruption within a system, an air force must have the ability to lift and project forces to areas of concern, and precisely insert and withdraw the required forces to accomplish the mission.

### Deny Sanctuary

The ability to reach anywhere around the globe denies sanctuary to any potential adversary. "You can run, but you can't hide" is the primary theme for strategic aerospace warfare. In the year 2025 strategic aerospace forces will influence the complete spectrum of war from Military Operations Other Than War (MOOTW) to nuclear, biological, chemical (NBC) operations. In denying sanctuary, the adversary leadership must understand that any potential strategic target can be "serviced" by aerospace forces. In the year 2025 physical sanctuary doesn't exist because of aerospace capabilities.

However, there are some potential shortfalls with the concept of sanctuary. The shortfalls that must be overcome may include political considerations, territorial integrity and neutrality, and "overflight" requirements.

Global Reach provides a means to reach and properly influence a strategic target. By "getting there" and exerting influence, the US achieves the desired impact on the adversary leadership's will. As an example, a terrorist base in a third-party nation or territory may be considered a viable target and we must be capable of providing the correct influence if called upon by our NCA. Recent examples include Hezbollah

terrorists' bases in Lebanon being struck by the Israeli Air Force. The dispute is not between Israel and Lebanon, but the territorial integrity of Lebanon must be violated for Israel to influence the "strategic" targets of the Hezbollah. Accordingly, the United States must be willing and able to work around the issue of territorial and airspace integrity of a neutral third party to deny sanctuary to our adversaries.

## Lift Capability

Global Reach in the year 2025 is required to provide a global omnipresence that is achievable through both close and remote influencing. Close influence is defined as the projection of forces into the theater. Close influence will require lift that is fast, rapidly transformable, and capable of moving outsized articles. Remote influencing is defined as influence performed on things outside the theater and usually requiring support from other instruments of power. Both types of influence will be conducted through a wide range of means, all with the intent of guiding the adversary's leadership to harmonize their objectives with our own. Thus, conventional forces, in some situations, will still be required to forward deploy to meet our national objectives. In the year 2025 lift will still be provided by traditional aircraft, and possibly augmented with transatmospheric vehicles (TAV) and ground-effect vehicles. In any case, strategic lift will remain the key element in providing global reach. Lift asset designs for 2025 must adhere to what they must transport. Thus the question: Who or what is going to require global transportation in the future?

## Lift Capacity

The two major regional conflicts (MRC) posture used today will not work in 2025. The year 2025 will require the NCA to understand and influence tens, maybe hundreds, or even thousands of different nodes in the global system to maintain harmony. The NCA will use many different forms of influence, but many challenges will require the use of the military instrument of power. Military ground forces will continue to require transport to areas where their expertise is required. Deployment of Air Force assets and their logistics tail necessary to operate the platforms of 2025 will also require transport. The forces deployed and the items brought to the region will be measured in the overall effect they have on changing the adversary's objectives. We must continue to provide a lift capability to project strategic influence to far-flung regions of the globe.

## Precision Insertion and Withdrawal

In 2025 equipment and personnel must be inserted and withdrawn precisely and timely. Lt Col John L. Cirafici, in his book *Airhead Operations: Where AMC Delivers*, proposes that

> the ideal situation for the supported combatant commander is for his forces to flow into theater airheads timely and be positioned where they are needed so that units can quickly and effectively reconstitute in anticipation of employment . . . while arriving forces are insufficient or relatively immobile, they can be destroyed by an opposing force. The airhead that the theater commander relies on for rapid introduction of forces and equipment is by its nature an area of vulnerability and, potentially, a bottleneck.[1]

Global Reach must have the ability to insert and withdraw forces precisely to reduce the vulnerability of conventional "airheads" and eliminate the associated bottlenecks. Precision insertion and withdrawal gives the combatant commander the flexibility of providing influence where and when needed in the least amount of response time. It is only through effective Global Reach that we can even consider the application of Global Power.

## Global Power

Power has been defined as "a psychological relationship between those who exercise it and those over whom it is exercised."[2] Power has also been defined as

> the ability of any actor to persuade, influence, force, or otherwise induce another actor to undertake an action or change an objective that the latter would otherwise prefer not to do. It is also the ability of one actor to persuade, influence, force, or otherwise induce another actor to refrain from an action that it would prefer to undertake.[3]

Power is an interesting concept since its perceived capability has as much as or more to do with its ability to influence an adversary than its actual capability. Also, power many times can take a form that is different from what we might expect. The announcement of the B-2 Stealth bomber to the world sent the USSR scurrying to understand the implications of an airplane that could fly undetected through their homeland. The cost of an air defense system capable of detecting the B-2 was far greater than they could afford. Their only solution, even though they had never seen a B-2, was to harmonize with our objectives and seek long-term peace. If a nation has both the will to use its instruments of power and the methods of employing its weapons, its position of power is elevated. The bottom line is the ability to influence an actor's strategic interests based on his perception of your capabilities, real or imagined!

## Perception Management

The intent of strategic aerospace warfare in 2025 will be to influence an adversary's leadership to harmonize with our objectives. The most effective method to do this will be through the subtleties of persuasion.

Persuasion is defined as "the process of preparing and delivering messages (through verbal and nonverbal symbols) to individuals or groups in order to alter, strengthen, or maintain attitudes, beliefs, values or behaviors."[4] The key words in this definition are messages, alter, strengthen, and maintain. Messages are sent to get someone or something to believe what you want. These messages can be in many different forms, but we shall focus on the mental aspects of messages in this section.

The US can either send a direct, truthful message to an adversary, or it can use deception in maintaining an adversary's perception of US intentions. In our opinion, the US must maintain and continue to develop a robust deception program that keys on the adversary leadership's understanding. According to Sun Tzu, "All warfare is based on deception."[5] But be aware as Attila the Hun stated, "One thing a chieftain should always fear more than doing battle is doing battle when only pretending to be prepared."[6] We must always be prepared to back up threats with action.

The key in prosecuting a successful deception program is the ability to attack the mind of the adversary while still having the ability to do battle. John Boyd's OODA loop[7] provides a model that demonstrates how deception can be used to strengthen and project power. Deception provides a very effective method of getting inside the cycle by disrupting the orientation portion. What is real? What is fake? What is the correct decision based on the information provided?

The vision of 2025—Global Awareness, Global Reach, Global Power all performed under the umbrella of information dominance will provide the framework for successful direction of the global system.

### Notes

1. John L. Cirafici, *Airhead Operations: Where AMC Delivers* (Maxwell AFB, Ala.: Air University Press, March 1995), 67–68.
2. Quoted in Daniel S. Papp, *Contemporary International Relations: Frameworks for Understanding* (New York: Macmillian Publishing Company, 1994), 28.
3. Ibid., 401.
4. Quoted in Gary C. Woodward, *Persuasion & Influence in American Life*, 2d ed. (Prospect Heights, Ill.: Waveland Press, 1992), 18.
5. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 41.
6. Wess Roberts, *Victory Secrets of Attila the Hun* (New York: Dell Publishing, 1993, 1963), 114.
7. David S. Fadok, *John Boyd and John Warden: Airpower's Quest for Strategic Paralysis* (Maxwell AFB, Ala.: Air University Press, February 1995), 16.

# Appendix B

There are many areas today that could begin to transform for 2025. By this we mean an ongoing study of contextual elements within the subregion to the region and finally to the theater level. The results of the theater analysis should be forwarded to a "notional" national agency that combines the results of the other commander in chief (CINC) studies to determine a global perspective that will provide guidance to make strategic decisions.

## Staff Flexibility

Theater-oriented CINC staffs should be organized for maximum flexibility and adaptability to handle the myriad of potential contingencies that may arise in 2025. The first step that needs to be taken is that all staffs everywhere adopt the organization of joint directorates.

> Unless there is learning and evolution taking place in how you go about doing knowledge work—in how you're organized to do it, how you handle knowledge, how you develop people, how you pay attention to the competitive environment—unless you're constantly getting better at all of these things and more, you're being sloppy, and there's a good chance that, eventually, you will find your organization falling behind.[1]

By instituting the joint directorate approach in all organizations, the flow of knowledge will have clearly defined paths. The J-5 of one organization should talk to the J-5 of another organization. They must not in the future waste time trying to figure out the difference between XONO, XOXO, or XONB and what information needs to flow where. Once we have created the framework for knowledge work we can now look at the requirements for decision making in our organizations of 2025.

Mr Pasmore, in his book *Creating Strategic Change*, states that

> by the time people are ready to decide something, the knowledge work is over. Therefore, all of the attention that has been placed on organizational decision-making is in fact *mis*placed. The real knowledge work goes on long before the meeting at which the decision is made; and it tends to be a very messy, disorganized process, open to the full negative forces of human foibles and social dynamics. By the time the decision is framed, the battle is over; it's classic garbage-in-garbage out.[2]

To really affect the decision-making process, intervention and guidance must be inserted, "while the knowledge is still being developed."[3] To create an environment for effective decision making, the organization must be structured to maximize knowledge. We propose an organizational structure to maximize the potential of our leaders and planners discussed earlier.

## The Polynoetic Organization

The classic "J-staff" has many centers of knowledge, from J-1 through J-8. To improve integration and knowledge transfer while retaining accountability, the proposed organizational structure for 2025 is a polynoetic organization presented by Mr Pasmore and illustrated below.

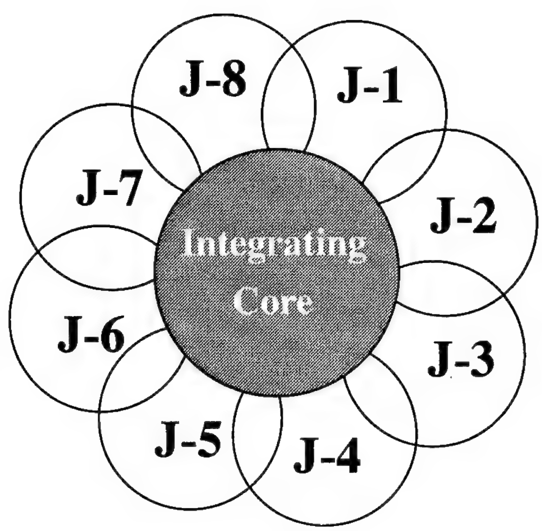



**Figure B-1. The Polynoetic Organization**

> The polynoetic organization is coordinated by a central group of knowledge workers who are themselves representatives of the various projects and activities undertaken by the organization. In addition, the integrating group contains individuals who represent administrative support functions . . . which provide information crucial to decision-making when such information is appropriate. In contrast to typical top management groups, the integration group has no stable membership or roles. The membership of the group varies upon the topics under discussion, the players heading up important projects, and suppliers of information relevant to the discourse. The integration group provides overall strategy guidance and allocates resources among competing demands. Leadership within the integration group rotates depending again on the knowledge demands of the ongoing and special deliberations on the agenda.[4]

This organization of a staff can be transformed for the occasion. This allows flexibility to adjust a staff based on the circumstances and unleash the power of the integrating core made up of the leadership corps. For example, a logistics-intense operation may require the J-4 to be the lead agent vice the J-3. An information-intensive operation may require the J-6 to be the lead agent. It also allows a multitude of projects to be coordinated simultaneously integrating the various outputs. The intent of this organizational structure is to allow a CINC the ability to mix and match knowledge within his staff to create effective decisions and direct appropriate influence on the global system.

Structure has a direct bearing on the effectiveness of a staff.

> The most important intervention to improve deliberation quality is to redesign the organization so that effective deliberations take place naturally, rather than fighting against improper structural influences. The organization design for effective deliberating takes into account the need to constantly realign knowledge with authority, yet integrate the outcomes of separate deliberations.[5]

Another key aspect is the overlap of functional areas. All the J-Staff functional areas should have some type of overlap or interactivity with the other J-Staff areas. These "liaisons" are critical in sharing knowledge among the directorates and may in fact be automated computerized filters that sort through the piles of information and direct it to the appropriate joint directorate based upon keyword, icon identification. In 2025 you no longer need to address where and to whom you believe your knowledge should go. Once it is created you just put it into the server and it is automatically routed to the appropriate agencies and anyone else who is pulling the data. We believe that to further enhance our ability to influence the global system properly, functions and duties within the joint directorates must expand.

## J-Staff Functions

We must begin today reorganizing and restructuring the staffs to prepare them to properly influence the nonlinear global system. Each J-Staff directorate should be organized along the lines of the polynoetic organization as explained in the body of this paper. This organizational structure is integral to maintain the efficient transfer of knowledge on the staff and within the directorate itself. In fact each directorate is set up as a system within a system.

For example, the J-1 directorate should have liaison cells that interact on a daily basis with the J-2 through J-8. This keeps the integrating core of J-1 informed on the activities of the rest of the staff and helps reduce friction within the directorate. Additionally, the functions of liaison should be rotated among the "action officers" to keep them abreast of the activities within the other directorates and how they function. This is critical in maintaining an educated core of staff officers that can perform within several areas of expertise if the need arises. Functions within the directorates themselves should be along the same lines as described in Air Force Systems Command Publication-1. However, we believe that some areas need to be explored in greater depth.

*J-1, Manpower and Personnel.* Current contingency planning requires manpower to "open" a unit type code (UTC) to determine the exact manning requirements for that

UTC. The manpower functional manager must coordinate with both the UTC functional manager and the Air Force speciality code (AFSC) functional manager to ensure proper manning for a contingency. This takes up more time than what should be considered appropriate. As 2025 approaches, manpower and personnel will have a critical function to deal with a smaller military. It will be essential that J-1 be the "lead agent" for *developing* force packages (manning levels) to deal with a contingency. However, the time for determining proper manning levels and coordinating through the functional areas must be done in a shorter amount of time than is done today. It would greatly enhance the planning process if the liaison cells for each functional area could report directly to a tasked unit for appropriate manning information. This becomes a critical concept when balanced against the possibility of a smaller Air Force and a smaller manpower base. The CINC-level planners must have the authority to deal directly with other CINCs to pull the appropriate manpower to deal with a contingency.

*J-2, Intelligence.* The emphasis of this directorate should remain on the "enemy." However, greater emphasis should be placed on identification and contextual understanding of potential strategic targets within the global system (e.g., how they could be influenced and what type of feedback would be required to measure success in influencing those targets). The directorate should be divided into theater, region, and subregion teams. These teams should undertake a comprehensive analysis of contextual and operational elements for their area of responsibility on a daily basis (using a bottom-up approach from the subregion to the theater level). These teams must have a direct link to any other US intelligence agencies (Central Intelligence Agency, Defense Intelligence Agency liaison, etc.) for a complete analysis of their assigned areas. Key to success in this area will be the successful fusion of the enormous amount of information available through filters to create true knowledge. We recommend the consolidation of as many "intelligence" agencies as possible to flatten the intelligence community. Will there really be a requirement for the CIA in 2025? What is the function of intelligence between a CINC staff and the CIA? Where does DIA fit into the equation? What is the purpose of the Naval Intelligence Command (NIC)? We believe that intelligence is intelligence, regardless of who is providing it. Information must be shared, otherwise it is useless. Get rid of the compartmented intelligence agencies and start basing intelligence on subregion to region to theater and finally to global for proper analysis. The coordination process is the most important aspect of planning. Based on the information provided by J-2, strategic targets can be identified prior to the onset of hostilities and effective means of servicing those targets can be coordinated by the other directorates.

Another important aspect of the J-2 should be feedback, or measuring success. A method must be determined before the onset of hostilities whether the selected influence is having the desired effect on the leadership's strategic aims. Access to all source information and monitoring adversary leadership positions on their original versus current courses of actions must be accomplished, and we believe it is the J-2 role to do this. It is crucial that an effective measure of an adversary's reactions be in place. By placing pressure on the adversary's strategic interests, the J-2 should be able to report probable or possible courses of action the adversary leadership may take. Once an action is taken by the adversary, it should be measured against the "desired" course of action and a resultant change in our strategic targeting should take place. This is the key element in prosecuting strategic warfare.

*J-3, Operations.* This directoract directs and controls current operations. Its work

begins with the initial planning and extends through the integration and coordination of joint operations. J-3 may be charged with the conduct of special operations, including psychological operations and special warfare, joint training, and coordination of joint exercises (AFSC Pub 1). Aerospace, land and sea components fall under the J-3 during contingency operations. These components must be able to identify capabilities for accomplishing the mission and conducting employment operations. To enhance the capabilities of the J-3, we feel some aspects of planning require drastic improvements to reduce planning cycle times and to display graphically the end results of a "plan." These improvements include functional experts who can quickly identify requirements and a graphics display board.

Personnel requirements include properly trained functional experts who can rapidly identify weapon systems to accomplish the desired mission. These experts should have the functional expertise to determine which UTCs are required for mission accomplishment. They should be operationally oriented experts who have a broad knowledge in their respective fields of expertise (e.g., fighters, airlift, spacelift, engineering, support, etc.). The intent is to rapidly identify requirements for a CINC to accomplish a mission. Time is the essential factor to maintain information dominance and disrupt an adversary's OODA cycle. These requirements should be graphically displayed on a planning board for a visual presentation for the planning staff.

Technical requirements include a 3-D holographic planning board that displays a from-theater-to-subregional view of the "battlespace." This should be applied to a "laptop"-type device with a window format to enhance deployment, employment, and redeployment planning. A window-in-window format would expand the area of emphasis showing possible beddown locations, terrain, strategic targets as determined by the J-2, enemy integrated air defense systems threat rings, global projection drop zones, and so forth. Once forces have been identified for deployment and beddown locations have been identified (using a "drag and drop" system with a movement priority identification system), the board could be used to wargame an ATO or campaign to deconflict packages while viewing the battlespace. This system would enhance the commander's overall view of the battlespace and graphically display the big picture. After witnessing the joint planning tool and other "systems," it would make sense to fuse the displays to provide this information. However, it is becoming evident that technology is enabling the concept of centralized execution. This area needs further examination for future commanders and war fighters.

*J-4, Logistics.* This directorate develops logistics plans and coordinates and supervises supply, maintenance, repair, evacuation, transportation, construction, and related logistics activities. Responsibilities may include weapons surety, civil engineering support, transportation management, and so forth. Because logistics support is a service responsibility, the primary thrust of joint logistics operations may be to coordinate service programs and integrate them with the joint commander's concept of support. Knowledge of service policies and doctrine is essential (AFSC Pub 1). J-4 must be responsible for theater distribution of both manpower and equipment and not the components. They should also be responsible for determining all strategic lift requirements to move assets into their respective theater (based on the apportioned lift). The J-4 must have a system (comparable to the J-3 holographic planning board) in place that will display all friendly fielded forces that are involved in operations. This system should provide the J-4 the ability to provide a view of the battlespace for the purpose of updating deployment, sustainment, and redeployment operations through the use of all-weather, precision delivery of supplies, manpower, and equipment.

*J-5, Plans.* This directorate does the long range planning. It prepares campaign, concept, and operation plans and the associated commander's estimate of the situation. Often, the J-5 is responsible for special weapons planning (AFSC Pub-1). The J-5 should be organized into theater, region, and country teams to analyze contextual elements and create the appropriate oplans/conplans/functional plans and time-phased force deployment data (TPFDD) plans. These teams should interface with J-2 teams and J-8 teams for comprehensive understanding of their areas of responsibilities. Additionally, the J-5 should be intimately involved in the acquisition process. All actions will have a strategic impact and the acquisition process will have major ramifications on the overall balance of strategic influence. The group in J-5 that would have inputs to the acquisition process would be performing the functions of a joint requirements oversight council/joint warfighting capability (JROC/JWCA) assessment team at the CINC level.

*J-6, Command, Control, Communications, and Computer Systems ($C^4I$).* The functions of this directorate include handling command responsibilities for communications and frequency control, tactical communications planning and execution, and management and development of electronics and automatic information systems to include hardware, software, and connectivity. It ensures interoperability with the services (AFSC Pub-1). The J-6 should be the CINCs' lead agent for information warfare. J-6 personnel would be the experts of both hardware and software to prosecute information warfare. Based on the inputs from the other directorates, the J-6 would be able to execute.

*J-7, Interoperability.* This directorate should ensure joint operations are coordinated. Functions should also include Deception and Black programs. The J-7 would ensure these compartmented programs are integrated into any operation. Any "special" tasked mission should be run from the J-7 directorate. This directorate should have a secure facility that houses a special mission control area that would provide connectivity to any platform tasked to perform special missions. These missions would remain out of the public eye and could be planned, controlled, and executed from this facility. The J-7s from all the CINCs would require a special category (SPECAT) message system to ensure unity of effort for all operations and connectivity to the national level agency.

*J-8, Resources (Civil Agencies).* Liaison cells organized in the same manner as the J-2 would greatly enhance the interoperability of the military functions with all nonmilitary agencies and organizations. Interaction between and with international nongovernmental organizations, international governmental organizations, international private organizations, Department of State, and the military becomes crucial. Staff members should become expert liaisons with political institutions such as the United Nations, civilian institutions that may have economic instruments that may be useful to a CINC, and so forth, especially in view of the MOOTW aspect of operations that may become more prevalent.

## Notes

1. William A. Pasmore, *Creating Strategic Change: Designing the Flexible, High-Performance Organization* (New York: John Wiley and Sons, Inc., 1994), 162.
2. Ibid., 158.
3. Ibid., 159.
4. Ibid., 166.
5. Ibid., 165.

# Bibliography


Cirafici, John L. *Airhead Operations: Where AMC Delivers.* Maxwell AFB, Ala.: Air University Press, March 1995.

Clarkson, Albert. *Toward Effective Strategic Analysis.* Boulder, Colo.: Westview Press, 1981.

Clausewitz, Carl von. *On War.* Edited and translated by Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1976.

DeBlois, Maj Bruce M. "Deterministic Philosophical Assumptions in the Application of Chaos Theory to Social Events." Unpublished paper. Maxwell AFB, Ala.: School of Advanced Airpower Studies.

Doughty, Robert Allan. *The Breaking Point: Sedan and the Fall of France, 1940.* Hamden, Conn.: Archon Books, 1990.

Drew, Col Dennis M., and Dr Donald M. Snow. *Making Strategy, An Introduction to National Security Processes and Problems.* Maxwell AFB, Ala.: Air University Press, August 1988.

*Encarta 95.* Microsoft, 1995.

Fabyanic, Lt Col Thomas A. *Strategic Air Attack in the USAF.* Research report no. 5899. Maxwell AFB, Ala.: Air University Press, April 1976.

Fadok, David S. *John Boyd and John Warden: Airpower's Quest for Strategic Paralysis.* Maxwell AFB, Ala.: Air University Press, February 1995.

Gilster, Herman L. *The Air War in Southeast Asia: Case Studies of Selected Campaigns.* Maxwell AFB, Ala.: Air University Press, October 1993.

Joint Publication 3-0. *Doctrine for Joint Operations.* 1 February 1995.

Keaney, Thomas A., and Eliot A. Cohen. *Gulf War Air Power Survey Summary Report.* Washington, D.C.: 1993.

Mowbray, Dr James A. "Air Force Doctrine Problems: 1926–Present." *Airpower Journal* 9, no. 4 (Winter 1995).

Myers, Isabel Briggs. *Introduction to Type.* Palo Alto, Calif.: Consulting Psychologists Press, Inc., 1993.

Papp, Daniel S. *Contemporary International Relations.* New York: Macmillan College Publishing Company, 1994.

Pasmore, William A. *Creating Strategic Change.* New York: John Wiley & Sons, 1994.

Penrose, Rodger. *The Emperor's New Mind.* New York: Oxford University Press, 1989.

_____. *Shadows of the Mind.* New York: Oxford University Press, 1994.

Richards, Chet. *Modeling and Analysis or Strategy and Decision?* Marietta, Ga.: Lockheed Corporation and the Georgia Institute of Technology, 1991.

Roberts, Wess, PhD. *Victory Secrets of Attila the Hun.* New York: Dell Publishing, 1993.

Sun Tzu, *The Art of War.* Translated by Samuel B. Griffith. London: Oxford University Press, 1963.

Szafranski, Col Richard. "Neocortical Warfare? The Acme of Skill." *Military Review,* no. 11 (November 1994).

Toffler, Alvin, and Heidi Toffler. *War and AntiWar: Making Sense of Today's Global Chaos.* New York: Time Warner, 1993.

*The United States Strategic Bombing Surveys: European War, Pacific War.* Maxwell AFB, Ala.: Air University Press, October 1987.

Warden, Col John A. III. "Air Theory for the Twenty-first Century." In Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future: 21st Century Warfare Issues.* Maxwell AFB, Ala.: Air University Press, September 1995.
Woodward, Gary C. *Persuasion & Influence in American Life.* Prospect Heights, Ill.: Waveland Press, Inc., 1992.

# Interdiction: Shaping Things to Come

Col Charles B. Oltman
Maj William T. Davidson, Jr.
Maj Steven S. Kempf
Maj Thomas K. Moore
Maj Theodore P. Ogren

## Executive Summary

Interdiction, based on the core competencies of precision employment and information dominance will still be used to shape the battle space in 2025. The critical pieces of these core competencies—accuracy, lethality, target identification, and cycle time—will necessarily undergo great change in the next 30 years. The result of these changes will be interdiction with a different face but the same heart. Interdiction in 2025 will require affordable enhancements to current capabilities in the areas of accuracy, lethality, target detection/identification, and timeliness, allowing the war fighter to shape the battle space in revolutionary ways.

A number of technological "leaps" will drive these required changes. Penetrating sensors and designators, coupled with microtechnology, will permit weapons to have the processing power required to "touch" targets in exactly the right spot. Variable lethality will permit the option of killing, delaying, deterring, or breaking targets. Synergistically combining these capabilities with intelligent system logic processing, improved target detection, decreased sensor-to-weapon cycle time, and airpower will provide the necessary pieces to dominate the battle space.

Among the systems required to build the interdiction system of systems in 2025 are beyond-electromagnetic sensors; acoustic, penetrating, and variable-yield weapons; sensory netting; energy and particle weapons; and a virtual observe, orient, decide, and act (OODA) loop. From these systems, a nexus of three enabling technologies emerges. If pursued, these technologies will provide the leveraged investment necessary to revolutionize interdiction. These technologies include: nanotechnology for inertial measuring units, sensors, transmitters, processors and locomotion; nonlinear modeling and intelligent systems to support the virtual OODA loop; and expanded use of the electromagnetic spectrum for weapon guidance and remote sensing.

# Chapter 1

# Introduction

*Air operations conducted to destroy, neutralize, or delay the enemy's military potential before it can be brought to bear effectively against friendly forces at such a distance from friendly forces that detailed integration of each air mission with fire and movement of friendly forces is not required.*

—Joint Publication 1-02

*In a time of drastic change it is the learners who inherit the future. The learned usually find themselves equipped to live in a world that no longer exists.*

—Eric Hoffer

*And all your future lies beneath your hat.*

—John Oldham

Interdiction has been around as long as airplanes. From the early attempts at "delaying" the enemy in World War I (WWI) by releasing bombs from open cockpits to pre-Normandy battlefield preparation to dropping laser-guided 2,000-pound bombs on unsuspecting Iraqi tanks at night, the desired result has always been the same—to "destroy, neutralize, or delay the enemy's military potential." These interdiction tasks have historically been accomplished by killing the enemy and/or blowing up their equipment before they get to the fight—in essence, shaping the battlefield. This has not changed.

To be effective, the air warriors in WWI, World War II (WWII), and the Gulf War had to perform very similar tasks. The airmen had to find the target, deliver the weapons accurately, and ensure adequate lethality to accomplish the desired level of destruction. And they had to do these three things in a timely manner. This also has not changed.

The period from WWI to the end of WWII covered a little less than 30 years. From the end of WWII to the Gulf War was another 45 years. During both of these periods, the ability to accurately deliver lethal munitions on target in a timely manner grew tremendously (fig. 1-1). What will the next 30 years bring?

Based on our core competencies of precision employment and information dominance, and pushed by the explosive growth and potential of technology, the face of interdiction will change, but not its heart. Interdiction in 2025 will require affordable enhancements to current capabilities in the areas of accuracy, lethality, target detection/identification, and timeliness, allowing the war fighter to shape the battle space in revolutionary ways. In describing these changes, this paper will define the required capabilities, describe the system components, detail a conceptual system that incorporates these components, and propose high-yield areas to investigate.

Although many discoveries could apply to battle space shaping in other mediums, the focus of this paper will be nonnuclear land interdiction. Additionally, as we examine interdiction, a logical line of questioning is, Why does this conceptual system only do interdiction? Why not strategic attack? What about close air support? What is unique to the interdiction mission that limits this system's application? The answer

to the final question is, Absolutely nothing! As our battle space awareness increases, the artificial lines that divide the battle space will continue to fade. This interdiction system can be effectively employed throughout the entire spectrum of attack operations, from strategic attack to close air support.

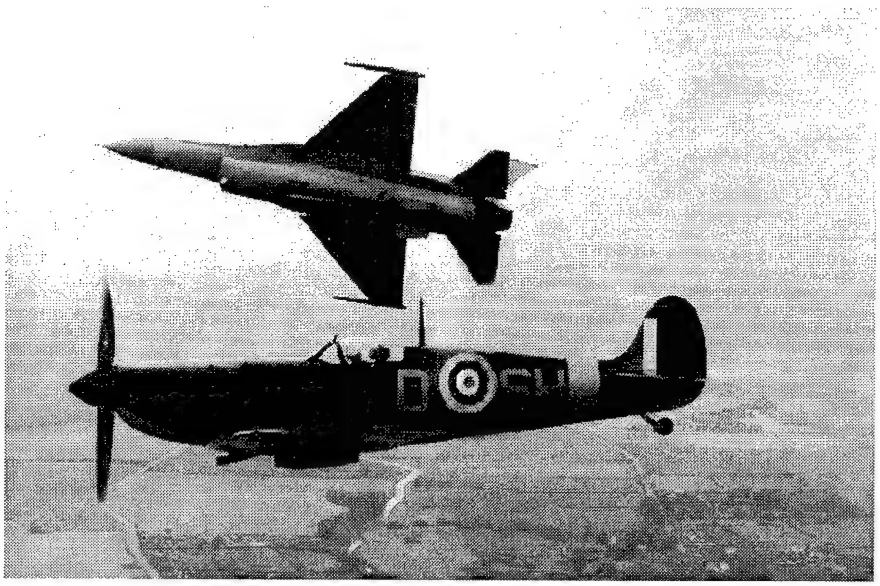


Photo Courtesy of Air Education and Training Command Photo Archive

**Figure 1-1. View of the Past**

## Chapter 2

# Required Capability

This chapter examines the capabilities airpower must provide for the interdiction mission of 2025. In broad terms, the required capabilities fall into two of airpower's core competencies: precision and information dominance. Precision, the ability to achieve specific desired effects, rests on the two pillars of accuracy and lethality. The second core competency—information dominance—stems from correct target detection and identification coupled with compressed sensor-to-shooter cycle time.

By 2025, hostile forces will have learned from our current capabilities and, as a result, they will adapt their systems and tactics to survive. The expanded 2025 interdiction arena, which includes conventional war, military operations other than war (MOOTW), weapons of mass destruction (WMD), counterproliferation, theater missile defense (TMD), and counterdrug operations, will be extremely challenging. For example, the target could be a small group of nonuniformed, lightly armed people walking through a jungle or through a city. Or the target could be fast, stealthy, armored vehicles, massed or dispersed. The 2025 interdiction system will engage such targets and meet those challenges.

The interdiction system in 2025 is characterized by force qualities based on the following basic tasks: detect, identify, decide, engage, and survive. The interdiction system of 2025 must excel at performing these tasks. A general sampling of the force qualities for these tasks includes but is not limited to coverage, timeliness, accuracy, availability, survivability, completeness, speed, resolution, stealth, range, optimum lethality, decision quality, and reliability.

In layman's terms, the interdiction system must do a variety of things well. First, it must achieve a complete and correct picture of the battle space. Next, it must perform the proper action to achieve the desired results. Both of these things must be done in an adverse and countermeasured environment.

The correct picture will be an accurate understanding of the location and movement of people and equipment in the designated battle space. Additionally, coverage of a significant geographic area could be needed for major contingencies. Coverage will vary by scenario, but tens of thousands of square kilometers could be needed. The density of coverage is also critical. Sensor sample density need not be spaced to the centimeter. However, distances as close as hundreds of meters between samples might permit important features of the battle space to be missed. Similarly, because different sensors detect different things, multispectral and/or multiple sensor types are needed. Finally, it is critical that the enemy system be modeled with sufficient fidelity to enable accurate prediction of hostile actions and reactions.

The enemy is a living, breathing organism that reacts to our actions. Col John Boyd, fighter pilot and renowned thinker, envisioned a way to conduct war based on OODA quicker than that enemy.[1] A key to employing this OODA loop effectively is to better anticipate the effect of an "act" on the enemy—and precisely placed ordnance enhances that ability to anticipate. Decreased cycle time, coupled with precision, permits the warrior to "get inside" the adversary's OODA loop and dictate the course of the battle. Col John Warden, another airpower strategist, echoed this sentiment when he stated, "They [precision weapons] change the nature of war from one of probability to one of certainty."[2] To Colonels Boyd and Warden, the term

"precision" meant more than just being accurate. Precision in this context meant being able to use a weapon in such a manner as to cause a predicted, desired effect for the purpose of advantageously shaping the battlefield. Clearly, interdiction in the future will require even more accurate and lethal munitions delivered in a timely manner.

The defense budget today is not growing. There is no reason to believe this will change by 2025. With an aging population and possible bankruptcy of Social Security, there will be great pressure to spend dollars on social services rather than military equipment. Therefore, any money spent on airpower will have to be evaluated on a strict cost/benefit basis. While this is not a required capability *per se*, affordability in 2025 will be a driving factor.[3]

## Mission Task Requirements

Precision and information dominance—accuracy, lethality, detection, and cycle time—will allow airpower to shape the battle space. Rapid advances in technology push us to improve our systems. While not disregarding such advances, we must seek innovative capabilities and operating concepts which will pull technology forward. We must identify key requirements which, if met, will provide us the tools to achieve national security objectives in 2025. What must airpower in 2025 do to delay, disrupt, destroy, and divert hostile personnel, materiel (vehicles, weapons, supplies), and communications? The required capabilities in precision and information dominance must accomplish the following tasks:

Delay Personnel and Materiel: To stop people from moving, our system must be able to incapacitate personnel, destroy/incapacitate their vehicles, obstruct/make unusable the routes of travel, or convince them they don't want to make the trip.

Disrupt Personnel and Materiel: Sow confusion (command, control, communications, computers, and intelligence [$C^4I$] interference, psyops), force the enemy to take actions of higher priority than moving.

Destroy Personnel and Materiel: Lethal attack to attrit unit to point of inability to function productively, destroy organizational integrity, and sufficiently damage critical materiel or render it useless.

Divert Personnel and Materiel: Induce them to move in a direction beneficial to us or give them a problem to solve which takes them from their intended course of action. Create a need for the materiel somewhere else, or induce the logistic system to send the materiel to the wrong place.

The system or systems required to carry out these interdiction tasks in 2025 will be comprised of personnel, organizations, delivery platforms, weapons, sensors, command and control systems, communications infrastructure, and support. In time of war or conflict, these resources must form a system able to destroy, disrupt, delay, or divert modes of transportation such as vehicles, roads, railroads, bridges, communication links, and even people. The system must operate in all environments: urban, jungle, desert, day, night, and in adverse weather. It also must be supported with timely intelligence and prioritization. The system will have to survive against a constantly evolving threat.

To perform these tasks adequately, the future interdictor will demand a broad range of options. The "emerging means of denial"[4] range from sticky foam and sonic guns to lasers and high-powered microwaves, but those are evolutionary advancements. This paper focuses on the revolutionary requirements—improvements in accuracy, lethality, target detection, and cycle time—which will lead us to the capabilities for interdiction in 2025.

## Accuracy

Tomorrow's weapons, such as the joint direct attack munitions (JDAM) and the joint standoff weapon (JSOW), will autonomously guide to within 10 meters, whether day or night, and in adverse weather. The weapons of 2025 will need to be significantly more accurate.

How much more accurate? “A reporter for the *New Republic* was in Baghdad the night of the first [Gulf War] air strike and the following morning watched smoke pour out of the Iraqi defense ministry. He was amazed that the hospital next to it was untouched as were the homes surrounding the ministry.”[5] With the ability to surgically remove a building from a city, what benefit is even greater accuracy? In Vietnam, news broadcasts brought the war to every American household by showing the death, destruction, and human suffering of civilians and soldiers alike. In the Gulf War, news broadcasts were live as the fighting occurred. Mass media continues to bring wars closer to the public. Ravages of war have always worked against public opinion. By increasing accuracy, airpower will continue to decrease collateral damage, helping prevent the loss of public support.

Today, we can skillfully remove a building within a city. By 2025, we may need the ability to strike specific offices, computer rooms, or command posts deep in the bowels of buildings without destroying the entire building. Enemy forces will no longer be able to hide among the civilian populace, endangering innocent lives. During the Gulf War, airpower inadvertently destroyed a fallout shelter for civilians which was collocated with a command post. The precision munitions/sensor combination of 2025 will need the ability to see inside the structure, penetrate various floors and walls, and detonate in the desired location. The result? One destroyed command post with few or no civilian casualties in the fallout shelter. Similarly, bridges could be dropped with a single bomb if it could exactly hit the main spar. The bomb yield could be smaller and collateral damage limited. This level of precision requires accuracy measured in centimeters rather than meters.

## Lethality

Improved accuracy will help us obtain greater lethality. But what is lethality? Lt Col Edward Schantz defined “the essence of combat lethality” as “[t]he ability to rapidly deploy an overwhelming force, target precisely, inflict maximum destruction with the minimum of assets, attack a wide range of targets nearly simultaneously to paralyze the enemy, and to suffer and inflict the minimum number of casualties.”[6] Another source took a slightly different view, describing lethality in two degrees, hard kill and mission kill.[7] A hard kill completely destroys the intended target along with any nearby people. In contrast, a mission kill disables the equipment permanently or destroys supplies while sparing human life in the vicinity. Additionally, future interdiction in some instances must have the ability to prevent enemy mission accomplishment while preserving life and infrastructure.

Fulfilling this requirement for variable lethality will permit airpower to effectively interdict in nontraditional arenas such as MOOTW, WMD counterproliferation, and TMD. The targets in these areas demand a wide range of lethality. Furthermore, in both these and conventional missions, we may need to preserve infrastructure (keep bridges standing, railroads functioning, etc.) yet still delay, disrupt, divert, or destroy. Limiting collateral damage is a driving concern in executing military operations today, and this trend will only increase.

## Target Detection and Identification

Rapid target detection, identification, and endgame decision making to optimize weapons effects will be equally important. Knowledge of seemingly insignificant characteristics of the battle space will be necessary. How else will the war fighter be able to predict, with an acceptable degree of certainty, the effect of his actions on the battle? This requirement demands sensors capable of operating across and outside the electromagnetic spectrum. Processing capability at the scene will be necessary to screen out unwanted data and identify

items of interest as well as discern friend from foe and neutral bystanders.

## Cycle Time

Systems which gather prescreened data should be capable of rapid information collection, knowledge enhancement, picture-building for the operator, and efficient dissemination of targeting information. With cycle times reduced to minutes or seconds, the only way to improve exploitation of the adversary's OODA loop is to accurately predict his movement in relationship to the battle space. But the battle space is, by definition, chaotic, requiring nonlinear modeling. The side that is able to employ vast computational power, with algorithms capable of simulating the chaotic nature of events as they unfold, will achieve information dominance.

Emphasis on accuracy, lethality, target detection, and cycle time as viewed by the Joint Chiefs of Staff[8] and senior Air Force leadership is at an all-time high.[9] Current trends in these areas show great promise. The required capabilities for interdiction in the 2025 battle space demand revolutionary technologies.

**Notes**

1. Maj David S. Fadok, "John Boyd and John Warden, Air Power's Quest for Strategic Paralysis," thesis for School of Advanced Airpower Studies (Maxwell AFB, Ala.: Air University Press, February 1995), 13–21.

2. John A. Warden III, "Air Theory for the Twenty-first Century," in Dr Karl P. Magyar et al., *Challenge and Response, Anticipating US Military Security Concerns* (Maxwell AFB, Ala.: Air University Press, August 1994), 327.

3. USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 5.

4. Frederick R. Strain, "The New Joint Warfare," *Joint Forces Quarterly,* Autumn 1993, 21.

5. Lt Col Thomas P. Mahoney et al., "Vulnerability Analysis of the United States," Air University Library Doc M-U 43122 M2161v (Maxwell AFB, Ala.: Air Command and Staff College, 1995), 21.

6. Lt Col Edward T. Schantz, "Combat Lethality: A Formula," Air University Library Doc M-U 43117 S229c (Maxwell AFB, Ala.: Air War College, 1994), 19.

7. Report of US Army Strategic Defense Command, "Theater Missile Defense Lethality Sensitivity Assessments" (Huntsville, Ala., July 1993), 1–5.

8. Adm William A. Owens, "Emerging System of Systems," *Military Review,* May–June 1995, 15–19.

9. Department of the Air Force, *USAF Executive Guidance,* January 1996.

# Chapter 3

# System Description

A description of required systems will help the reader envision the technologies to be developed. This section will focus on systems for accuracy, lethality, target detection/identification, and cycle time.

## Accuracy

Airpower stewards of 2025 should focus on three technologies—laser modulation, molecular recognition, and microsensors—to improve weapon accuracy.

Laser modulation will offer two advantages. The first advantage is the ability to penetrate a structure in a nondestructive inspection and the second is the ability to designate an exact point inside the structure, thereby guiding a penetrating munition to a precise detonation point within that structure. Laser devices generate a coherent beam by using a light source to excite atoms of a crystal, liquid, or gas medium. As the light is agitated in the crystal, liquid, or gas medium, it is reflected by mirrors. The reflected light agitates more atoms, generating more light of the same wavelength. Eventually, the light will build to such an intensity that it will overcome the reflectivity of one mirror and spill out of the laser device in a beam of coherent light. The crystal, liquid, or gas used for the lazing medium will determine the frequency and wavelength of the laser beam. Currently, there is a laser device that can modulate its frequency. It is called a "dye laser." The "tuning range can . . . be extended into the ultraviolet at the shorter end and into the infrared at the longer-wavelength end"[1] (fig. 3-1).

The energy generated in the light frequency range between microwave and ultraviolet offers only a slight amount of penetration capability. More simply, energy in the light frequency will reflect off the outside or external part of the structure. Energy in the microwave region can penetrate some materials, but will reflect off others. As the frequency or wavelength of a lazing beam changes throughout the spectrum, its ability to penetrate moisture, smoke, haze, or even solid objects, improves. This is similar to using an X-ray machine to see inside a person's body. "The power of X-rays for penetrating matter increases as the wavelength decreases."[2] By modulating the frequency throughout the

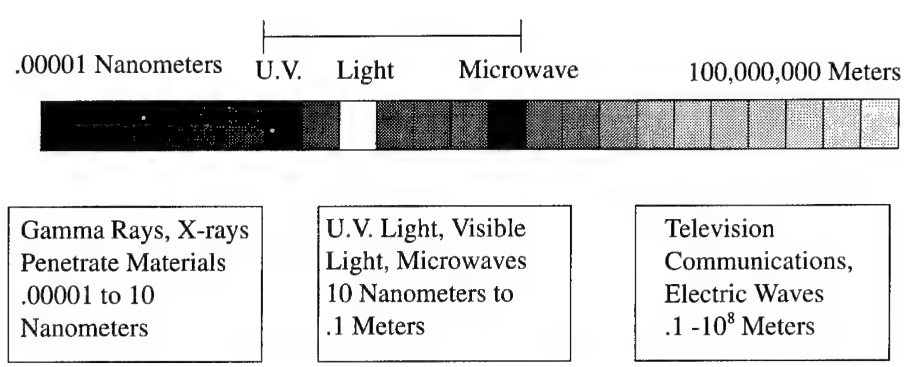



**Figure 3-1. Present-Day Dye Lasers**

entire electromagnetic spectrum, the device could control the frequency to penetrate or to reflect off of the various materials comprising the structure. From a database of material properties, a computer would analyze the different wavelengths based on parameters such as intensity of reflected energy, lack of reflected energy, or a shift in phase of the wavelength. Using this analysis, the computer would build a three-dimensional image of the structure and display it to the weapon operator. For example, a laser modulating weapon could examine a structure like a bridge and show the weapon operator a three-dimensional image of the internal skeleton of the structure. This would allow the weapon operator to locate the main spar and guide a weapon to an exact point inside the structure, thereby dropping the bridge with an explosive power the size of a stick of dynamite (fig. 3-2).

Lazing a target may be impractical—a more autonomous system might be needed to attack a target. Some view autonomous weapons as the next challenge in improving weapons. One visionary research paper from the Army Command and General Staff College stated, "Brilliant munitions, currently in the notional [conceptual] state, will combine the autonomous operation of smart munitions with enhanced navigation and targeting classification and identification capabilities."[3] Classification and identification will be discussed later; this section will focus on autonomy. The heart for these weapons is the inertial navigation unit (INU). Today, INU errors grow by rate of time squared.[4] That is to say, inaccuracy increases at an exponential rate after initial alignment. To maintain an accurate INU, the system can be updated in-flight by different systems such as the global positioning system or terrain-imaging systems. Updating the INU provides another vulnerability to the system. Future autonomy will come in making the INU more accurate. Historically, the inertial measuring system in the INU was a spinning mass gyro which evolved to a laser gyro.

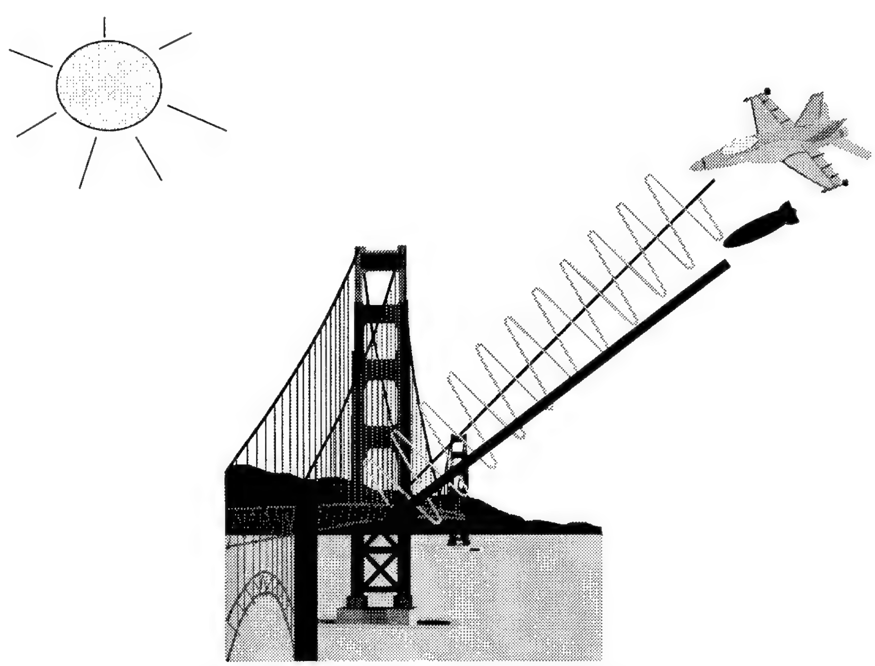


Figure from Microsoft Clipart Gallery © 1995 with Courtesy from Microsoft Corporation

**Figure 3-2. Laser Modulating Weapon**

The INU of the year 2025 could be a nuclear gyro. Utilizing radioactive *molecules*, the INU will measure the smallest of changes. Orientation and acceleration will be accomplished by multiple buckeyballs (Buckminster Fullereen molecules) containing radioactive, specially shaped nanoparticles.[5] The INU will never drift to an inaccurate state, and updating will be unnecessary. This will decrease vulnerability and provide pinpoint accuracy.

Autonomy is a great asset for stationary targets, but defining the endgame coordinates of a moving target significantly increases the level of difficulty. One approach supposes a datalink from the target to the weapon. A self-contained datalink module will attach itself to a target and transmit information to the weapon. The envisioned device will be miniature. It will have the ability to sense the composition of the target and to fuse with the target, so it cannot be removed. After fusing, the sensors will begin transmitting data, such as direction, speed, composition of material, armament, personnel on board, vulnerabilities, and other useful information to a weapon sensor. The device will transmit the information to a central computer. The computer will analyze it and other information transmitted from other targets, display a three-dimensional picture, and prioritize targets for commanders to analyze. After the commander decides which targets to attack, the computer will determine the most vulnerable point and the size of yield, and will guide the weapon to the exact point of vulnerability within the target. Improvements in miniaturization of power sources, sensors, and computers will be required.

## Lethality

The word "lethal" connotes destructive power "capable of causing death."[6] In the spirit of reducing collateral damage and attaining specifically desired affects, weapons in the year 2025 will vary through a spectrum of lethality—from total destruction to target destruction without death to merely delaying or disrupting target function.

> America's national science laboratories are among those who recognize this reality [varying lethality] and are currently theorizing, developing, and testing these next generations of weapons, thereby transcending the precision guided munitions (PGM) used in the gulf war. Nonlethal technologies are the only way to fully exploit telecommunications [as well as other targets], and depending on campaign objectives, they may be cheaper, more effective, and less destructive.[7]

Regardless of the level of lethality, weapons in the year 2025 will require technological advances in target penetrability and variable yield.

Weapons will have differing penetrability characteristics in 2025. This section will explore acoustic devices that prepare targets for kinetic energy weapons to penetrate; energy or particle beam weapons that penetrate structures directly; and a revolutionary concept, weapons that bore into structures.

Most weapons today use kinetic energy to penetrate a target. It could be costly in redesign efforts and arsenal replacement to design harder, higher-velocity weapons. A more likely scenario for kinetic weapons in the next 30 years is to use the same weapons as today but prepare the target for penetration. In other words, soften the target prior to bombing it. Materials are collections of bonded particles. A device that could break down those bonds would enable kinetic energy weapons to penetrate more easily. One way to weaken these bonds is to generate a resonating frequency in the structure. A sound-producing device imbedded in or attached to a target could send sound waves throughout the structure. A computer in the device would analyze the structure and adjust intensity and frequency until the structure resonates. "The amplitude of forced oscillations becomes exceptionally large whenever the driving frequency is near a natural frequency (resonating frequency) of the vibrating body."[8] These oscillations would weaken the material in the structure, thus allowing kinetic energy weapons to

penetrate more easily. Although power requirements may be substantial, several of these devices working together would be able to add to the output without causing an increase in power demands per device.

Energy or particle beam weapons penetrate by translating through materials as described above. If enough energy were added, the beam could be a destructive force itself, like a laser scalpel used in surgeries today. Limited power sources and collateral damage would restrict the use of this weapon. However, several distinct energy or particle beam weapons focusing on the same point could individually penetrate structures without harm and cause internal damage at the designated point (fig. 3-3).

These weapons could be self-contained, in orbit around the earth, and networked to a control facility either in orbit or on the ground. There are three advantages: (1) they would not individually do anymore harm to the environment than microwave stations do today; (2) the system would be difficult to kill; and (3) the individual energy or particle beam systems could easily be disguised as communication satellites. This system would require a lens with zero defects to provide very accurate aiming and limit beam attenuation. Toward solving this, Dick Siegel, a scientist at the Renssalear Polytechnic Institute, has developed a way to manipulate matter on an atomic level.[9] He would essentially build the lensing medium atom by atom. Such homogeneous materials would provide precise focusing, enabling the energy or particle beams to converge precisely, providing maximum energy at a given point.

Penetration can also be achieved by boring to the desired point. Too often we envision weapons that do all their work in a split second of time, explode, and are gone. But a weapon that could bore through any material would not have to work quickly; nor would it have to explode. This concept envisions a weapon that would work like a furniture worm. These worms bore through furniture, weakening it to the point of collapse. A bore weapon would ingest the material as it bored. The ingested material would be broken down by chemicals and enzymes. Useful molecules could be used for energy and the rest discarded. It would be very small, and many of them could

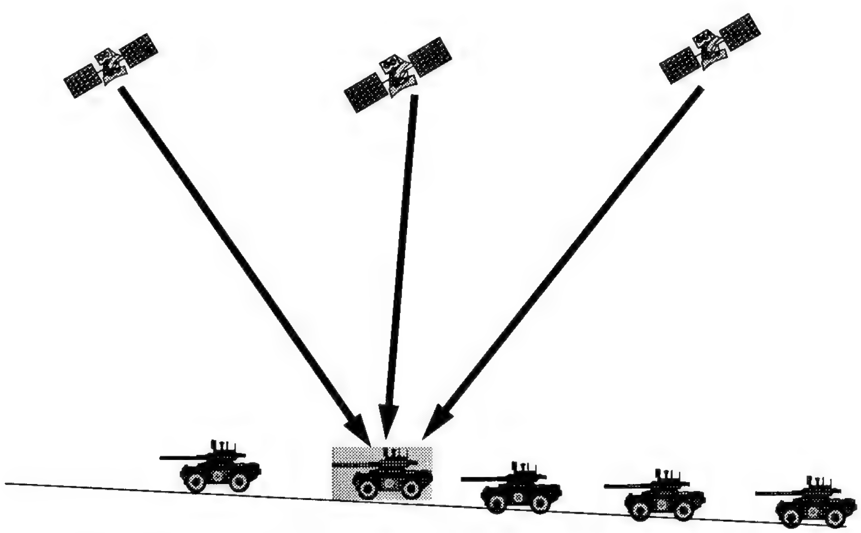


Figure from Microsoft Clipart Gallery © 1995 with Courtesy from Microsoft Corporation

**Figure 3-3. Multibeam Attack System**

infest a target. They could be linked to a central control system so as to work in unison and reach the most vulnerable spot quickly; or they could be disabled by the touch of a button if the enemy conceded to demands. Technological advances in computer miniaturization and chemical decomposition would be paramount.

If a weapon can accurately target inside a structure and penetrate to that point, then the final step is to apply the appropriate force to attain the desired effect. Energy or particle beam weapons of the year 2025 will adjust their yields by adjusting power output. Explosive weapons, however, cannot as yet adjust their explosive yield—it is a fixed parameter based on the explosive fuel in the bomb. The advantage of adjusting the yield lies in providing the most possible flexibility to the tip of the sword. An airplane, for example, with an adjustable yield weapon could be diverted from destroying a bridge, which might take a 100-pound yield, to destroying a communications room, which might take a 10-pound yield. This example shrinks the OODA loop, minimizes collateral damage, and provides the most flexibility to the war fighters. This section will examine two concepts for adjusting the yield on a weapon: metamorphic material and beam activation of materials.

Explosive weapons today use chemical compositions that, when ignited, burn at a rate and pressure inherent in the type of materials used.

> All chemical reactions are accompanied either by an absorption or evolution of energy, which manifests itself as heat. It is possible to determine this amount of heat and thus the temperature and product composition from the very basic principles. Spectroscopic data and statistical calculations permit one to determine the internal energy of a substance. The internal energy of a given substance is found to be dependent upon its temperature, pressure and state and is independent of the means by which the state was attained.[10]

Therefore, by being able to change the material composition of the weapon, one could instantaneously adjust the yield of the weapon. The concept for a metamorphic material is to develop a substance that could change its molecular structure. An electrical charge of varying voltages could be the catalyst for changing the composition of the material. A charge would cause one chemical in the explosive solution of the bomb to alter its molecular bonds, thus changing into a different solution and generating a different yield. A charge of a different voltage would make a different explosive solution with a different yield.

The concept of beam activation is similar to the metamorphosing materials described above; however, in this instance, the ordnance penetrates to the exact point required but does not detonate. A beam of energy is then applied to the ordnance from an airborne or spaceborne platform to trigger ignition. The type of energy beam will determine the yield of the explosion. For example, a microwave beam would activate chemicals in the solution different from those of an X-ray beam. Activation of different chemicals in the explosive solution would realize different yields.

## Target Detection and Identification

> There is radiance and glory in the darkness, could we but see; and to see we have only to look. . . . I beseech you to look.
>
> —Fra Giovanni[11]

> The trouble with people is not that they don't know but that they know so much that ain't so.
>
> —Josh Billings[12]

Historically, target detection and identification have been sequential and loosely associated processes. Targets were detected by various means (visual, radar, infrared), located, visually identified, and finally engaged. Initially, our ability to engage a target was limited because of our inability to detect and locate targets. Increasingly, however, our ability to detect, locate, and engage has greatly outpaced our ability to identify. All of the long-range detection and engagement systems in the world are worth nothing if we cannot

correctly and confidently identify the targets. As we move into the future, the speed, and consequently the ranges, at which we will need to engage will increase significantly. Furthermore, the targets and target environments of 2025 will provide much greater challenges. We will be required to detect weapons of mass destruction at long ranges. We will need to operate in urban environments. In order to successfully meet these challenges, future systems will precisely detect, locate, identify, and "know" how best to attack the enemy. This "knowing" will use a greatly expanded range of brilliant sensors, mounted on a wide variety of platforms and networked together to fuse all of the information into widely available target knowledge.

We detect most ground targets by using the electromagnetic spectrum, either optically (using the visual or infrared spectrum) or electronically (by either radar reflection or passive emission detection). The likely proliferation of stealthing and camouflaging techniques will reduce either the effectiveness of current detection systems or our confidence in those systems. Since stealthing is usually only effective in specifically targeted regions of the electromagnetic spectrum, we must expand the range of the spectrum our systems use for target detection.

Currently, lasers are used almost exclusively as designation systems to guide munitions. By 2025, advances in laser technology will permit reflected laser energy to be processed not only to determine target location and classification, but also to build a picture of the target for positive identification purposes. Furthermore, by using laser technology identified previously in the accuracy section, these sensors will be able to look beyond the surface and into the heart of a target. This will provide additional data for target identification and decoy rejection—stealthing and camouflage will be rendered useless.

Sensors have inherent limitations associated with their operating frequencies. For example, visual systems have good resolution but cannot see through weather or in the dark; infrared systems can see in the dark but are limited by weather; millimeter wave radar works in bad weather and darkness but has poor resolution.[13] Multispectral imaging, capturing images of a given target, by using different regions of the electromagnetic spectrum and combining those images, can overcome the limitations associated with any particular region of the electromagnetic spectrum. Furthermore, not only are natural limitations overcome, but camouflage as well. A tank that is covered with branches may look like a bush, but it still has the thermal footprint of a tank. While it would be possible to disguise the tank further with thermal camouflage, it would still have the radar signature of a tank. For every camouflage short of actually building another tank, some region of the electromagnetic spectrum will reveal the camouflage.

By 2025, multilayered semiconductors and new polymeric materials will be designed and processed at the atomic level.[14] "These new materials will make possible sensors with high sensitivity across the entire electromagnetic spectrum, data transmission links with greater than 200 gigabits per second, parallel processing of data at breathtaking speeds, three dimensional data storage with almost instantaneous access."[15] Not only will these new materials "see" more; they will be able to compile multiple images much faster. Multispectral imaging will give way to hyperspectral and ultraspectral imaging. There will be fewer and fewer places to effectively hide (fig. 3-4).

Furthermore, sensors in 2025 will not only use more of the electromagnetic spectrum; they will move detection outside of the electromagnetic realm entirely. Scientists are developing intelligent materials that will be able to bond with objects and distinguish material characteristics of that object. Ultra thin layers, 200 to 300 microns thick, of piezoelectric polymers—like polyvinylidene

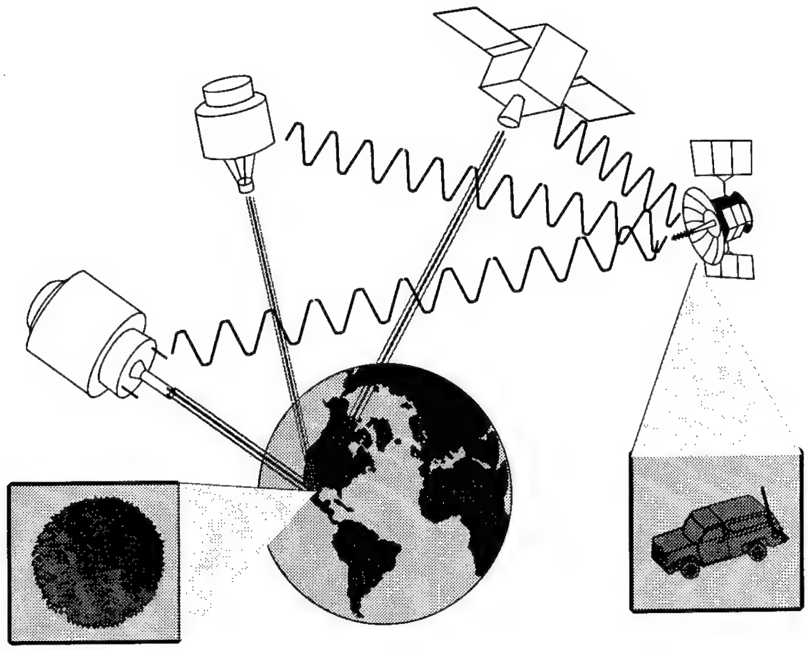


Figure from Corel DRAW!© 1992 with Courtesy from Corel Corporation

**Figure 3-4. Multispectral Imaging**

fluoride (PVDF) in particular—are very sensitive to texture, temperature, and shape.[16] Sensors using these materials will be able to "taste" and "feel" targets. Furthermore, chemists are working on developing spectrometers that are the size of handheld calculators.[17] These battlefield sensors will be able to sense the environment by looking for proximate target indications like exhaust fumes while miniature acoustic sensors will be "listening" for targets. These systems would be able to "smell" and "hear" targets!

Evolutionary improvements in computational power and artificial intelligence applied to all sensor systems will lead to revolutionary improvements in performance. These systems will become "brilliant" sensors. They will be able to perform in-depth analyses of all available data and compare the results against a vast library of cataloged threat systems and friendly systems. Having analyzed the data to such a level, the sensors will be able to provide information not only on target location and identification but also on target vulnerabilities. This will permit the tailoring of force to precisely affect the target.

To enhance their utility, these sensor systems will be located on an almost infinite variety of platforms in space, in the atmosphere, and on the surface. Any form of aviation platform will be able to support a sensor suit covering the entire range of detection capabilities. Surface sensors can be either fixed or deployable. Fixed sites will approximate something like the distant early warning (DEW) line of old, while increased processing capability will reduce the size and cost of such installations. Reductions in size and power requirements will permit sensor deployment on multiple small satellites, clustered together on large satellites, or clustered on a space station.

The area that shows the most promise for revolutionary advances in sensor technology is nanotechnology. Miniature electronic and mechanical machines can be combined and manufactured through use of the lithography techniques currently found in computer chip production. These devices,

called microelectromechanical systems (MEMS), are sized on the order of hundreds of microns.[18] Advances in computers will also provide powerful processing capacity to a single integrated chip.[19] Similarly, advances in memory devices will permit a trillion bits of information to be stored on a single chip.[20] Combining this powerful computing capability with the MEMS devices will allow us to deploy the "taste," "smell," "feel," and "hear" sensors directly to the battlefield as a "swarm" of "miniature unattended ground sensors" (MUGS). The MUGS could be air-dropped in the neighborhood of a supply chokepoint and become a remote sentry reporting on enemy activity. As enemy equipment approaches, the MUGS detect the equipment, identify the equipment and its contents, and report the information.

Finally, massive intelligent networking of all sensor systems will permit the widest possible dissemination of target knowledge (fig. 3-5).

As any individual sensor detects a target, it not only turns its full analysis capability on that target; it also identifies that target to other sensors for analysis of different modalities. All of the sensors will report their findings to intelligence networks for further analysis and possible targeting. As weapon systems are employed against these targets, the sensors will help guide munitions and optimize the effects of those munitions, as well as report munitions effects providing combat assessment. The MUGS, however, will require revolutionary advances in power and communications technologies to be able to communicate beyond their immediate environment. Short of solving these long-range communication problems, it would be possible to make the MUGS "smart" reflectors. Having locally determined the nature of a target, the MUGS would alter their state so that an energy beam reflected off them would contain meaningful target information. Passing aircraft, satellites, or other systems

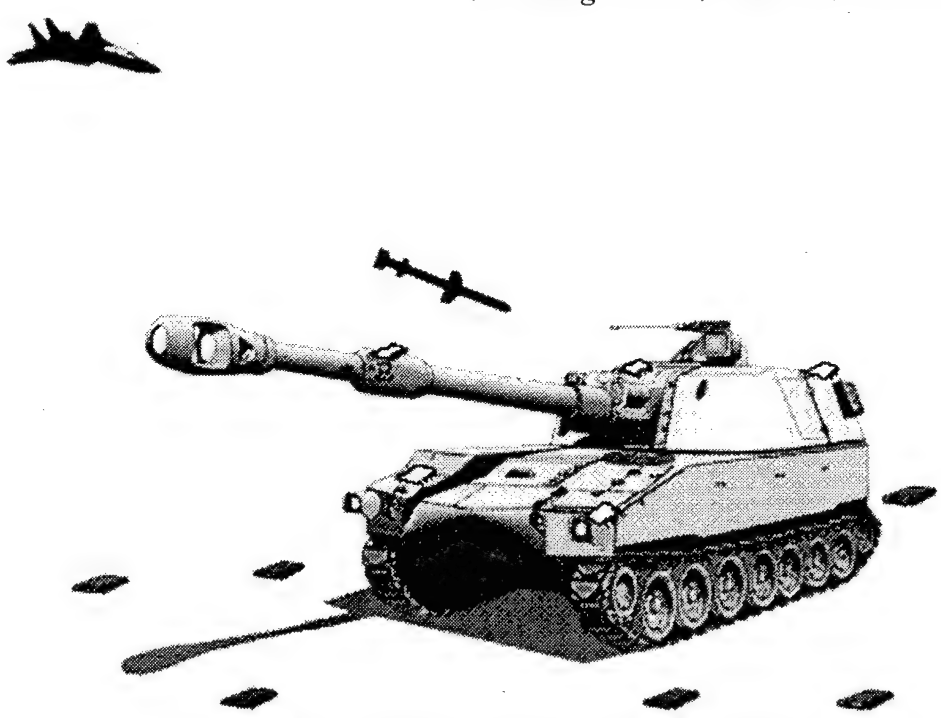


Figure from Corel DRAW!© 1992 with Courtesy from Corel Corporation

**Figure 3-5. Miniature Unattended Ground Sensors (MUGS)**

would be able to poll the MUGS by scanning them in passing.

Regardless of whether the MUGS are delivered by a transatmospheric vehicle, an unmanned aerial vehicle (UAV), or the Good Humor man, they will require insertion on the battlefield. While it is impossible to know at this point precise dimensions or capabilities of the MUGS, some rough calculations will give us an idea of coverage we can expect. Given that the MEMS that are currently being developed have dimensions on the order of hundreds of microns, it is not unreasonable to assume that a MUGS of 2025 with a complete suite of communications and power capabilities, camouflage, and either motive or adhesive systems would be one centimeter square by one millimeter thick. A generic delivery canister of one cubic meter capacity would hold 10,000,000 sensors. If these sensors can reliably detect targets and communicate with each other at a distance of one meter, this one container could distribute enough sensors to cover an area approximately three kilometers on a side. If the range of the MUGS is increased to 10 meters, the area is 30 kilometers on a side or 900 square kilometers.

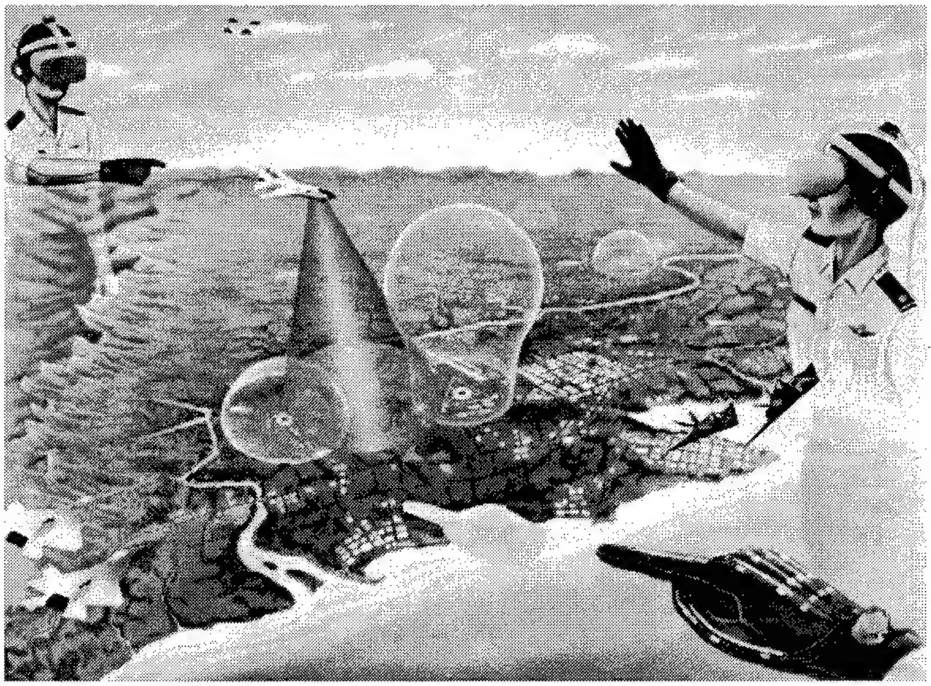
The MUGS would be ideal for detecting weapons of mass destruction and operating in urban environments. Properly configured, MUGS will be able to detect smaller evidence of WMD, more precisely locate the WMD, report WMD movement and determine the status of the environment after an attack to destroy the WMD. MUGS placed throughout an urban environment will permit more accurate tracking of targets in that environment. MUGS programmed to detect language, cultural, and equipment differences, placed in a building in which terrorists are holding hostages, would be able to determine the number, location, and status of both terrorists and hostages. Rescue attempts would be more effective, with greater likelihood of success and fewer friendly casualties. Substitute enemy soldiers in a city and similar results can be anticipated.

## Cycle Time

Cycle time, within the context of targeting for interdiction, has historically followed a cycle of "detect, decide, and destroy."[21] Although the Air Force has chosen to embrace a newer version of the decision-making process in Boyd's previously mentioned OODA loop, the process still requires events to occur before new data can be input as the observe portion of the cycle. Increasing the tempo of operations by reducing cycle times makes the employed force appear larger to the enemy. The goal of the commander is to repeat the cycle as rapidly as possible to minimize losses and maximize effect.

To maximize the effects of weapon systems in 2025, the ability to predict possible courses of action for commanders will be required. The ability to model the battle space and explore options before actually executing them will allow analysis to determine best effects for least cost. Consider a military forecasting system capable of predicting enemy actions from 12 to 24 hours in advance and offering courses of action for evaluation. Using chess as an analogy, the commander will be able to predict the outcome of his third move, knowing the result of the second, while the first is taking place. Such a system, perhaps using a 3-D holographic battlefield display[22] or a battle space awareness holosphere,[23] would allow commanders to plan interdiction sorties against centers of gravity for the upcoming enemy operation (fig. 3-6). In the holographic interface system, the battle space is projected in a three-dimensional format so all aspects of the battle can be interpreted by the commander.

To get additional information on a particular area or target, the commander zooms in or simply touches the object. Full details are then immediately available. If full details are not present, the system interprets the "touch" as a request;



Picture Courtesy of Air Force Institute of Technology

**Figure 3-6. Holographic Interface**

additional sensor information is then sought. The holographic system would incorporate imagery, terrain information, air defense information, knowledge of the opponent's tactics, treaty implications, and all sensor data from the target detection/identification network. The database for the system, pervasive and distributed, draws from many sources around the world. Some possible inputs to the database include Central Intelligence Agency data, Department of State analyses of governments and engineering data on the opponent's system. The holographic system will have call-up panels for other $C^4I$ tasks. For example, to establish a link with a commander at another center, the operator will touch the appropriate unit's symbol and a video-conference link will be established with the other commander. The system would project the battle space at the level of detail requested by the commander, and providing a real-time view of enemy and friendly forces. The ability to simulate attacks on various enemy targets, inflict damage to friendly forces, and view the results are integral parts of a battle space awareness system. By using the system to analyze the effects of attacks on both sides of the battle, future commanders will be employing a "virtual OODA (VOODA) loop." The VOODA system and its three-dimensional modeling of the battle space requires understanding. Concepts such as nonlinear modeling and intelligent systems must be developed.

Nonlinearity, for the purpose of this discussion, is defined as an aperiodic equilibrium state of a dynamic system. A system in nonlinear equilibrium seems to wander randomly, yet the behavior is deterministic. If you know the equations, you can predict in advance any point of the nonlinear path or trajectory.[24] The problem is in understanding how to model battle space as the behavior becomes complex. Complex behavior implies complex causes. Events that are seemingly unpredictable, like a battle, are governed by many independent controls (such as individual commanders) or by random external influences

(like weather).[25] Modeling a complex scenario requires a choice—either make the model more complex and more faithful to reality, or make it simpler and easier to manage. The simpler model is easier to produce and requires less understanding of all the complex factors involved, but will provide less useful results over time.

To tie this concept to battle space planning, consider the current means of weather prediction. Complex algorithms and supercomputers produce a forecast with reasonable accuracy for a 12- to 24-hour period; however, the farther into the future the model predicts, the less reliable the forecast. Currently, computing power struggles under the load of complex algorithms and the multiple iterations necessary for long-term accuracy. In 2025, predicted computing capability will give increased accuracy by allowing more complex algorithms to forecast events.

The data and software necessary for a VOODA loop system will be staggering, as will the required computing capability. The software that drives the system requires an adaptive "intelligent system" approach. An intelligent system implies multivalued or "vague" logic, or, simply put, "everything is a matter of degree."[26] An intelligent system learns rules from data or by watching the behavior of human experts through a network of sensors. The system with the greatest potential for military use is the fuzzy cognitive map (FCM) computer. An FCM draws a causal picture by tying facts, assumptions, and processes into values, policies, and objectives. It is designed to predict how complex events interact and play out.[27] An FCM has concept nodes and causal links. Concept nodes are vaguely defined sets like "tanks on a road" or "strength of a bridge." Causal links are vague rules that connect the nodes to show the effects of one node on another. FCMs thrive on feedback to determine which nodes are changing and by how much. The sensors of the future battle space will provide the necessary data to the FCM. Intelligent systems are currently used in adaptive process controllers, air-fuel mixture ratio controllers, and automatic transmissions.

These and other areas of military and commercial applications could gain order of magnitude improvements. By allowing the commander the option of stepping forward in time, FCMs using developed intelligent systems and simulation techniques offer great promise for improving cycle times in 2025. The ability to select the third move, based on the results of the planned second move, while the first move is taking place, represents an astounding improvement in cycle time. According to Noboru Wakami, a Matsushita engineer, "[intelligent systems are] like seasoning. Sometimes the seasoning simply improves the taste [of food]. Sometimes it produces something dramatically different."[28]

## Summary

The interdiction mission in 2025 will require significant technological "leaps" to achieve the required accuracy, lethality, target detection, and cycle time. Penetrating sensors and designators coupled with microtechnology will permit weapons to have the processing power required to "touch" targets in exactly the right spot. Variable lethality will permit the option of killing, delaying, deterring, or breaking targets. Add intelligent system logic processing, improved target detection, and decreased sensor-to-shooter cycle time to these capabilities and the result is clear—airpower will dominate the battle space.

### Notes

1. Hrand M. Munchenyan B. SC., E. E., M. SC., *Principles and Practices of Laser Technology* (Blue Ridge Summit, Pa.: Tab Books Inc., 1983), 96.

2. Charles F. Meyers, *The Diffraction of Light, X-rays, and Material Particles* (Ann Arbor, Mich.: J. W. Edwards, 1949), 284.

3. "Fundamentals of Smart Weapons," Appendix 1 to Advance Sheet, Meeting 4, Report no. A304-4 (Fort Leavenworth, Kans.: US Army Command and General Staff College, September 1991), 82.

4. Gerald Frost, *Operational Issues for GPS-Aided Precision Guided Weapons* (Santa Monica, Calif.: RAND, 1994), 4.

5. ***2025*** Concept, no. 20014, "Molecular Inertial Navigation Sensor," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

6. *The American Heritage Dictionary* (Boston: Houghton Mifflin Co., 1982), 725.

7. Maj Gerald R. Hurst, *Taking Down Telecommunications* (Maxwell AFB, Ala.: Air University Press, September 1994), 29.

8. Donald E. Tilley, *Contemporary College Physics* (Menlo Park, Calif.: The Benjamin/Cummings Publishing Co, Inc., 1979), 454.

9. Robert Pool, "Atom Smith," *Discover*, December 1995, 56.

10. Irvin Glassman, *Combustion Second Edition* (Orlando, Fla.: Academic Press, Inc., 1987), 1.

11. Suzy Platt, *Respectfully Quoted, A Dictionary of Quotations Requested from the Congressional Research Service* (Library of Congress, Washington, D.C.: Government Printing Office, 1989), 274.

12. Ibid., 185.

13. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the sensors volume, 15 December 1995), 92.

14. *New World Vistas*, summary volume, 87.

15. Ibid.

16. Craig A. Rogers, "Intelligent Materials," *Scientific American*, September 1995, 124–25.

17. Gabriel J. Kaigham, "Engineering Microscopic Machines," *Scientific American*, September 1995, 121.

18. Ibid., 118.

19. David A. Patterson, "Microprocessors in 2020," *Scientific American*, September 1995, 49–50.

20. Kaigham, 120.

21. Capt Richard E. Nock, "High Payoff Targets: When to Engage," *Military Intelligence* 19, no. 2 (April–June 1993): 19–23.

22. ***2025*** Concept, no. 900385, "3-D Holographic Battlefield Display," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

23. ***2025*** Concept, no. 900417, "Battlespace Awareness Holosphere," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

24. Bart Kosko, *Fuzzy Thinking, The New Science of Fuzzy Logic* (New York: Hyperion, 1993), 288.

25. James Gleick, *Chaos, Making a New Science* (New York: Penguin Books, 1987), 303.

26. Kosko, 292.

27. Ibid., 222.

28. Ibid., 183.

## Chapter 4

# Concept of Operations

*We make war as personal as a punch in the nose. We can be selective, applying precisely the required amount of pressure at the specified point at a designated time—we've never been told to go down and kill or capture all left-handed redheads in a particular area, but if they tell us to, we can.*

—Robert A. Heinlein

Some of these areas of enhancement do not represent, by themselves, revolutionary ways of doing business. Nonetheless, from today's baseline, each of the individual attributes—accuracy, lethality, target identification, and cycle time—will experience exponential growth. What is revolutionary, like blitzkrieg,[1] is the way these exponentially improving elements will be combined to accomplish interdiction—the interdiction system of systems. What follows is a description, based on the technologies outlined in the previous section, of a global attack system (GAS) in the year 2025. Our system is composed of four key subsystems: (1) a battle space targeting system, (2) a networked sensor array, (3) a variable lethality, very smart weapon, and (4) a command, control, and communications system to tie these subsystems together.

Overseeing the entire interdiction system is "the man in the loop"—the joint force commander (JFC) and staff. The battle space system contains numerous information filters to provide the appropriate information to the appropriate level, but targeting authority belongs to the JFC. Since all the players have access to the same battle space data, the JFC has complete flexibility to delegate this authority based on the forces available, the campaign plan, and the desired effect on the enemy.

The brain of the interdiction system of systems is a targeting system.[2] The interdiction targeting process begins with the JFC, based on fused battle space information, designating an area of interest to the targeting module. This module, located in either space, an uninhabited reconnaissance air vehicle,[3] or an AWACS/JSTARS-like aircraft, collects data via multispectral imaging[4] and processes the data intelligently to identify potential targets of interest. After concurrence from the joint force air component commander (JFACC) or his designated representative, the targeting module initiates the launch of unmanned aerospace vehicles (UAV) that contain the miniature sensors.

These sensors are dispersed in the target area and begin to relay information to the targeting module. The JFACC, based on the sensor information received and the offensive game plan, designates the exact target and desired level of destruction. The targeting module then launches nearby fighters, bombers, or UAVs, gives them initial target information, and "hands them off" to the sensor array. The air vehicles proceed to the target area and drop their sensor-controlled weapons on the designated targets.

The eyes, ears, taste, smell, and touch of GAS comprise a miniature sensor array.[5] This sensor array is composed of adaptive microscopic machines that, having been dispersed by UAVs, seek out and find "interesting items." After attaching to items of interest, the sensors begin to talk to each other and form a network. As the network matures, it is able to determine what is a valid target and what is not, where the target's most vulnerable points are, what weapons effects will produce the best results, and where living beings are located.

The sensor array then relays this information to the targeting control system. This system now has enough information to match assets to targets, based on not only target type and destruction requirements but also on an assessment of collateral damage risk. Ultimately, the sensors pass some of this information directly to the weapon. Additionally, the sensor array is able to report level of destruction to the targeting control system, which can then update its target list and continue the process as required.

The business end of the GAS is the fist—the variable-lethality weapon.[6] This weapon, delivered by either a manned or unmanned platform, is the ultimate in sensor-to-weapon-linked technology with the ability to vary the effects of the weapon based on sensor input. Using the networked sensor array, a direct data link is established between the sensor and the weapon. This link serves two purposes. First, it provides exact location information to allow precise weapon placement. Second, using the information collected on the type of material and structure, the sensor adjusts the yield of the weapon to produce the desired level of destruction. For example, hard targets might require a higher yield, underground targets might require delayed fusing to allow penetration, flimsy aboveground structures might require an airburst to maximize blast, and so forth.

In addition to adjusting the bang, based on target requirements, the weapon is also able to flex to a nonlethal mode of operation. When the sensor array "notices" items whose damage or destruction would hamper the commander's strategic effort, the sensor-weapon link would reduce the yield and/or change the mode (e.g., blast to sticky ooze) based on preset or real-time operator inputs. One size truly fits all!

The final required element to allow GAS to function properly is a way to link the receptors, the brain, and the fist to one another, all under the control of the JFACC. We need a nervous system—a secure, high-speed, large bandwidth communication system—that will provide the required information flow. Although essential to our system of systems, this requirement is not unique to interdiction and is assumed to be in place.

The interdiction organism is now complete. It has a brain, an ability to sense its environment, a way to influence its environment, an ability to communicate amongst its various parts, and someone to tell it what to do. However, our interdictor can be rendered ineffective by attacking it at any of these points. The brain could be destroyed outright or infected with a crippling "disease." The eyes and ears could be "repelled" with an antisensor spray or, worse yet, information within the sensor net or from the net to the weapon could be altered (location, yield, etc.). The fist could be deflected or destroyed prior to target impact. The nervous system could be completely severed (electromagnetic pulse info weapon) or selectively disabled (spot jamming, etc.). All of these potential countermeasures will have to be considered and countered as we develop our "interdiction system of systems."

Having described the global attack system, a few caveats are in order. First, GAS is not delivery-platform dependent. As we progress toward 2025, new manned and unmanned platforms will be developed. GAS can be implemented on a variety of these platforms. Secondly, given the often uneven development of technology, advances in sensor technology may outpace that of variable-yield weapons. However, as pieces of GAS are completed, they can be implemented with a corresponding increase in capability. Finally, forward basing, if available in 2025, would improve the system response time. However, the impact of that decrease in response time is very situation-dependent.

Although GAS may do interdiction very well, a broader question must be answered. Does it answer the mail? Does this system satisfy the requirements identified for an

effective interdiction system in the year 2025? The short answer is, YES! The critical force qualities required in 2025 are all satisfied by the various subsystems in our interdiction system of systems. For a detailed snapshot of force qualities versus GAS elements, see table 1.

As you examine this interdiction organism, a logical question is, Why does this beast only do interdiction? Why not strategic attack? What about close air support? What is unique to the interdiction mission that limits this system's application? The answer is, Absolutely nothing! As our battle space awareness increases, the artificial lines that divide the battle space will continue to fade. This interdiction system can be effectively employed in the entire spectrum of attack operations, from strategic attack to close air support.

**Table 1**

**Force Qualities Summary**

| | GLOBAL ATTACK SYSTEM | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | BRAIN | | SENSORS | | FIST | | | |
| | Holographic Interface | FCM Computer | Multispectral Laser | MUGS | Nuclear IMU | Acoustic Prep Devices | Multibeam Attack System | Variable yield weapons |
| **DETECT** | | | | | | | | |
| Sensor Coverage | | | X | | | | | |
| Sensor Revisit Time | | | X | X | | | | |
| Location Accuracy | | | X | X | | | | |
| Environmental Availability | | | | X | | | | |
| Sensor Survivability | | | X | X | | | | |
| Unobtrusive | | | | X | | | | |
| Completeness | | | X | X | | | | |
| **IDENTIFY** | | | | | | | | |
| Speed | | | X | X | | | | |
| Accuracy | | | X | X | | | | |
| Resolution | | | X | X | | | | |
| Traceability | | | X | X | | | | |
| Battlespace View | | | | X | | | | |
| Correlation | | | X | X | | | | |
| **DECIDE** | | | | | | | | |
| Speed of Decision | X | X | | | | | | |
| Decision Basis Accuracy | | X | | | | | | |
| Decision Quality | X | X | | | | | | |
| **ENGAGE** | | | | | | | | |
| Range | | | X | | | | X | |
| Accuracy | | | X | X | X | | X | |
| Timeliness | X | | X | X | | | X | |
| Desired Lethality | | | X | X | X | X | X | X |
| Multirole (Flexibility) | | | X | X | | | X | X |
| **SURVIVE** | | | | | | | | |
| Vulnerability | X | X | | X | | | | |
| Countermeasures | X | X | X | | | | X | |
| Stealth | X | X | | X | | | | |

## Notes

1. Blitzkrieg was a revolution in military affairs that combined evolutionary technology in a revolutionary way to outpace the enemy in the battle.

2. ***2025*** Concept, no. 900859, "Space-Based Target Designator System," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

3. USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 21.

4. Ibid., 20.

5. ***2025*** Concept, no. 900860, "Neural Net Sensor Array," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

6. ***2025*** Concept, no. 900858, "Sensor-Controlled Weapons Effects," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

# Chapter 5

# Investigative Recommendations

This paper has identified a number of enabling technologies for the interdiction system of 2025. Some subsystems were highlighted: beyond-electromagnetic sensors; acoustic, penetrating, and variable yield weapons; sensory netting; energy and particle weapons; and a virtual OODA loop. From these, three technologies emerge. These are the critically enabling technologies which, if pursued, will provide the basis for an interdiction revolution. The first is nanotechnology for inertial measuring units, sensors, transmitters, processors, and locomotion. The second, nonlinear modeling and intelligent systems, will support the virtual OODA loop. The third is expanded use of the electromagnetic spectrum for weapon guidance and remote sensing.

Nanotechnology is critical because the sensing end of the system depends on it. To cover a meaningful geographic area, these sensor/processors must be produced in huge quantities at low cost. Industry, even now, produces vast quantities of such devices. One example is the microchip inertial measuring units produced for automotive airbag actuation. In the future, miniature mass spectrometers and "inexpensive chemical detectors" will be made.[1] Such machines could certainly be adapted to fill the sensing needs of our system. Built through use of microchip production techniques, these machines will easily possess the transmitters, processors, and receivers that the interdiction system requires.

As stated, this system will have the processing capability of modeling the battle space with the fidelity necessary to predict the effect of the war fighter's next move. Today, we can predict the weather for a 12- to 24-hour period. The nonlinear algorithms used for this, combined with vast processing power, will be available in 2025. Today, we must begin to expend the effort to study and understand the battle space in terms of chaos theory and fuzzy logic so its unique features can be modeled.

Exponential gains in computational and processing capability are necessary, but they will be a "given" in 2025. Individual computers in 2025 "will be as powerful as all those in silicon valley today."[2] Commercial enterprise over the next 30 years will provide substantial support for the development of nanotechnology and nonlinear modeling.

The third technology deemed critical is the expanded use of the electromagnetic spectrum. At first blush, this seems to have little industrial utility. Guiding a weapon to a precise location within a structure is not a peacetime pursuit, but unobtrusively examining the interior of a structure is commonly needed—for example, aging bridges require testing to determine their health. Perhaps mining and oil drilling operations could benefit from a CAT scan/magnetic resonance imaging (MRI) of potential sites.

## Conclusion

Nanotechnology for inertial measuring, sensors, transmitters, processors, locomotion, and nonlinear modeling, as well as intelligent systems for the virtual OODA loop and expanded use of the electromagnetic spectrum for weapon guidance and remote sensing, are the key interdiction technologies for airpower focus over the next 30 years. They are derived by envisioning required capabilities, describing systems that might be used in 2025, and then consolidating them into a concept of operations. These futuristic ideas were identified through the timeless core competencies of precision and information dominance. The great visionary, William Mitchell, once said, "In the development of

airpower, one has to look ahead and not backward and figure out what is going to happen, not too much of what has happened." This paper has looked ahead and offers direction to air and space professionals. All that is left is to act.

## Notes

1. Gabriel J. Kaigham, "Engineering Microscopic Machines," *Scientific American*, September 1995, 118–21.

2. David A Patterson, "Microprocessors in 2020," *Scientific American*, September 1995, 48–51.

## Bibliography

***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College, 1996.

*The American Heritage Dictionary*. Boston: Houghton Mifflin Co., 1982.

Department of the Air Force. *Executive Guidance*. January 1996.

Fadok, Maj David S. "John Boyd and John Warden, Air Power's Quest for Strategic Paralysis." Thesis for School of Advanced Airpower Studies. Maxwell AFB, Ala.: Air University Press, February 1995.

Frost, Gerald. *Operational Issues for GPS-Aided Precision Guided Weapons*. Santa Monica, Calif.: RAND, 1994.

*Fundamentals of Smart Weapons*. Appendix 1 to Advance Sheet, Meeting 4. Report no. A304-4. Fort Leavenworth, Kans.: US Army Command and General Staff College, 1991.

Glassman, Irvin. *Combustion Second Edition*. Orlando, Fla.: Academic Press Inc., 1987.

Gleick, James. *Chaos, Making a New Science*. New York: Penguin Books, 1987.

Hoffer, Eric. "Reflections on the Human Condition." In *The Columbia Dictionary of Quotations*, Columbia University Press, 1993.

Heinlein, Robert A. *Starship Troopers*. New York: Ace Books, 1987.

Hurst, Maj Gerald R. *Taking Down Telecommunications*. Maxwell AFB, Ala.: Air University Press, September 1994.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 1 December 1989.

Kaigham, Gabriel J. "Engineering Microscopic Machines." *Scientific American*, September 1995, 118–21.

Kosko, Bart. *Fuzzy Thinking, The New Science of Fuzzy Logic*. New York: Hyperion, 1993.

Mahoney, Lt Col Thomas P., et al. "Vulnerability Analysis of the United States." Air University Library Doc M-U 43122 M2161v. Maxwell AFB, Ala.: Air Command and Staff College, 1995.

Meyers, Charles F. *The Diffraction of Light, X-rays, and Material Particles*. Ann Arbor, Mich.: J. W. Edwards, 1949.

Munchenyan, Hrand M. *Principles and Practices of Laser Technology*. Blue Ridge Summit, Penn.: Tab Books Inc., 1983.

Nock, Capt Richard E. "High Payoff Targets: When to Engage." *Military Intelligence* 19, no. 2 (April–June 1993): 19–23.

Oldham, John. "Lines to a Friend About to Leave the University." In *The Columbia Dictionary of Quotations*, Columbia University Press, 1993.

Owens, Adm William A. "Emerging System of Systems." *Military Review* (May–June 1995): 15–19.

Patterson, David A. "Microprocessors in 2020." *Scientific American*, September 1995, 48–51.

Platt, Suzy. *Respectfully Quoted, A Dictionary of Quotations Requested from the Congressional Research Service*. Library of Congress, Washington, D.C.: Government Printing Office, 1989.

Pool, Robert. "Atom Smith." *Discover*, December 1995, 56.

Schantz, Lt Col Edward T. "Combat Lethality: A Formula." Air University Library Doc M-U 43117 S229c. Maxwell AFB, Ala.: Air War College, 1994.

Strain, Frederick R. "The New Joint Warfare." *Joint Forces Quarterly*, Autumn 1993, 21.

Tilley, Donald E. *Contemporary College Physics*. Menlo Park, Calif.: The Benjamin/Cummings Publishing Co., Inc., 1979.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century*. Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

USAF Scientific Advisory Board. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Sensors Volume. 15 December 1995.

US Army Strategic Defense Command. "Theater Missile Defense Lethality Sensitivity Assessment." Huntsville, Ala., July 1993.

Warden, John A. III. "Air Theory for the Twenty-first Century." In Dr Karl P. Magyar, et al. *Challenge and Response: Anticipating US Military Security Concerns*. Maxwell AFB, Ala.: Air University Press, 1994.

# Hit 'em Where It Hurts: Strategic Attack in 2025

Lt Col Jeffrey E. Thieret
Maj Frederick I. Guendel, Jr.
Maj Steven J. DePalmer
Maj Michael A. Silver

## Executive Summary

In the year 2025, advances in technology should allow air and space assets to affect an adversary anytime, anywhere. The ultimate goal of strategic attack is to conduct operations "to a point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity."[1] Employing a "hit 'em where it hurts" philosophy, 2025 strategic attack operations run the gamut from traditional, highly destructive, force-on-force encounters to much less invasive, but very effective, computer-based warfare.

The diverse nature of potential adversaries, and the vast amount of information pertaining to them, requires an integrated approach to protecting American and allied security interests. Technological advances will enable all levels of leadership to successfully deal with the vast volumes of information in ways not envisioned or realized in the past. These advances will make it possible to accurately determine and engage an adversary's Locus of Values (LOV). The LOV is that which an adversary holds dear, and which if influenced or threatened would affect the enemy's ability or will to carry out covert or overt aggression against the United States.

LOVs are hard or soft. Hard LOVs are physical things: militaries, weapons of mass destruction, or industries. Soft LOVs are intangible things: systems, knowledge, or ways of thinking. LOVs are engaged immediately or never, lethally or nonlethally, directly or indirectly. Each strategic situation is unique, yet in every case, the "force" applied against an LOV focuses on a strategic effect.

The key elements of strategic attack in 2025 are system analysis, target acquisition, target engagement, and feedback. Each phase is integrated and connected in virtual real time with the others through an organic integrated system directed to, and interpreted by, human decision makers.

#### Note

1. Department of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (draft) (Langley AFB, Va.: USAF Doctrine Center, 15 August 1995), 13.

## Chapter 1

# Introduction

Strategic attack in the ***2025*** program is both unchanged from what it has been throughout human history and yet radically different. How can this duality be true? The truth is found in the ends and means of strategic attack.

Across time, the objective of strategic attack has been to conduct operations that would have a war-winning effect on an adversary. We need look no further than proposed Air Force doctrine, which asserts that the goal of strategic attack is to conduct operations "to a point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity."[1] In other words, we are doing things that will affect the entire war, not just a particular target, battle, or campaign. Therefore, it is the end result of strategic attack that has not changed.

The part of strategic attack that has changed involves the means. The methods by which attacks are planned and conducted to produce strategic effects will be very different in 30 years. The leaping advance of technology, different ways of organizing these technologies, and evolving military doctrine guarantee that the means will change. Clearly, strategic attack is not about weapons—any weapon can be strategic if it affects the adversary's ability or will to wage war. Furthermore, the same weapon can be tactical, operational, or strategic, depending on its use and how it affects the enemy.

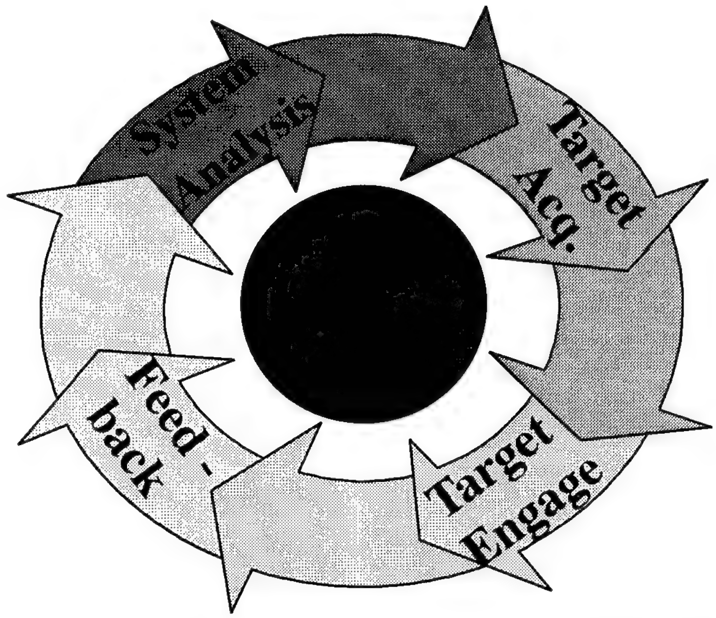
The key to strategic effect is the opponent's values. Every adversary is unique; therefore, every strategic attack will be different. This idea has been handed down through generations of warriors as the concept of a center of gravity (COG).[2] The term *COG* created a good image in an age of Lapacian determinism, where machinery was the model; however, in 2025 the view is more organic, so the COG concept loses some of its usefulness. A more descriptive term is LOV: that which is held dear and which, if influenced or threatened, would affect the enemy's ability or will to wage war or carry out aggressive activity.[3]

Armed with the term *LOV*, we turn to the wave metaphor of Alvin and Hiedi Toffler for a framework in which to conduct strategic thinking. The Tofflers' paradigm asserts that human societies are evolving upward in waves, rather than in a constant climb. The societal waves are split into three segments, based upon what drives the entity's economy: agriculture, industry, or information. Further, the values of each wave society differ from those which another wave holds dear.[4] The world in 2025 will contain societies rooted in each wave.

The Toffler model is useful to the warrior because it can be applied to a diverse range of potential adversaries. By using the wave model to ascertain the dominate societal focus of an adversary, one can gain insight into critical LOVs. With LOVs accurately determined, the samurai of 2025 can prosecute an effective strategic attack.

The Toffler wave model provides a point of departure for planning attacks.[5] It suggests that: (1) first wave adversaries are best dealt with by targeting individual leaders or territory; (2) second wave opponents will be threatened by destruction of armies or industry, and (3) third wave enemies focus on idea-centered technologies or economies.[6]

The wave model helps us think about what to attack to achieve strategic effect, which is but one part of the process. Knowing the correct LOVs must be




**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 1-1. Strategic Attack Process**

combined with acquiring and engaging them, and then determining if the attack was effective. This organic strategic attack process produces war-winning effects against an adversary. Figure 1-1 illustrates four key elements of strategic attack: system analysis, target acquisition, target engagement, and feedback.

Information links the above four elements of strategic attack. Information revolves primarily around the adversary's LOV, which eventually becomes strategic "targets" comprised of many dimensions. LOVs are either hard or soft. Hard LOVs are physical things: militaries, weapons of mass destruction, or industries. Soft LOVs are intangible things: systems, knowledge, or ways of thinking.[7] Both are engaged immediately or never, lethally or nonlethally, directly or indirectly. Each case is different, yet in every case the force applied is aimed at strategic effect.

**Notes**

1. Department of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (draft) (Langley AFB, Va.: USAF Doctrine Center, 15 August 1995), 13.
2. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, N.J.: Princeton University Press, 1976), 145–47.
3. For more information on targeting value, see Joseph A. Engelbrecht, Jr., "War Termination: Why Does a State Stop Fighting?" (PhD diss., Columbia University, 1992).
4. Alvin Toffler and Heidi Toffler, *War and Anti-War* (New York: Little, Brown and Co., 1993), 18.
5. Ibid.
6. Ibid., 21.
7. LOVs are broken into two categories: hard and soft. Hard LOVs are things that we can, and have throughout the history of warfare attacked physically. The thought process for this being that by hurting an enemy we can change his mind about fighting—an indirect path to war fighting. Physical attack is used as demonstration model in this paper because history has proven that it can work. Another approach is to attempt to directly influence an enemy by manipulating his thought processes or values. This is the essence of targeting soft LOVs. Owing to the unproven nature of this approach, and the fact that it is well covered in the Team E white paper, it is not elaborated on here.

# Chapter 2

# Required Capabilities

Strategic attack in 2025 requires certain capabilities. Some capabilities will evolve from current organizational doctrine and technology. Other capabilities require revolutionary developments, much different from current tools of strategic attack. The capabilities required for each element of strategic attack are categorized as shown in table 1.

**Table 1**

**Strategic Attack Requirements for 2025**

| Strategic Attack Element | Required Capability |
|---|---|
| System Analysis | Knowing the LOV |
| Target Acquisition | Locating the LOV |
| Target Engagement | Affecting the LOV |
| Feedback | Determining Results |

## System Analysis

In his pamphlet *10 Propositions Regarding Air Power*, Col Phillip Meilinger suggests that "In essence, Airpower is targeting, targeting is intelligence, and intelligence is analyzing the effects of air operations."[1] Knowing what to attack to achieve the desired effect is the critical element. Further, what to target varies greatly between adversaries. The LOV for a textbook second wave nation may be its industrial web. For a nation possessing a small military capability, yet wielding tremendous informational and economic might, the LOV may be their information infrastructure. For nonstate actors such as terrorist organizations, drug cartels, or organized crime syndicates, the LOV may be their leadership. In short, knowledge acquisition is particularly important in strategic attack because the aim is to impact across the whole of an adversary from highly focused inputs.

Knowing "what" to attack has always been difficult, and it will become harder in 2025 for a number of reasons. The first concern involves the growing number of actors. A burgeoning number of sovereign states, emerging transnational groups, multinational corporations, and other organizations will influence US policy. Next, add increased access to previous "close hold" information through the explosion of media, the Internet, and population migration. And finally, stir in a world political dynamic that is much more fluid than during the cold war. Because of all these challenges, the system analysis problem becomes incomprehensible to the unaided human decision maker.

The human decision maker's ability to determine strategic LOVs in 2025 will come from a combination of technologies. These include exploiting national and global databases, employing artificial intelligence (AI) technologies to turn that data into usable information, and using increased computational capacity to run the AI programs in a near-real-time fashion.

Exploiting data 30 years hence will certainly remain a daunting task. The USAF Scientific Advisory Board (SAB) addresses this problem in their *New World Vistas* study: "Much of the information which is needed to construct the global picture exists today in computers somewhere. The problems of the next decade are to identify the relevant databases, to devise methods for collecting, analyzing, and correlating them, and to construct the needed communication and distribution architectures."[2] Therefore, a critical enabling capability to conduct strategic

attack in 2025 is an ability to exploit all relevant sources of existing and emerging data.

Turning the acquired data into useful information for strategic decisions is the task of AI technologies. AI is a multidisciplinary field that aims to develop device technologies capable of solving problems in a manner similar to that of a human being. AI permits a computer to constantly comb vast amounts of data for useful kernels of seemingly unrelated data, process them into information, and then deliver that information to decision makers in a timely manner. Advanced AI is required to correlate the mountain of unorganized data located throughout the information domain.[3]

AI technology employs sophisticated computer programs. By its nature, AI requires large amounts of computational ability and storage capacity. Current hardware meets the needs of today's AI applications; however, by 2025 AI applications will require faster processors and much larger data storage capacities.

## Target Acquisition

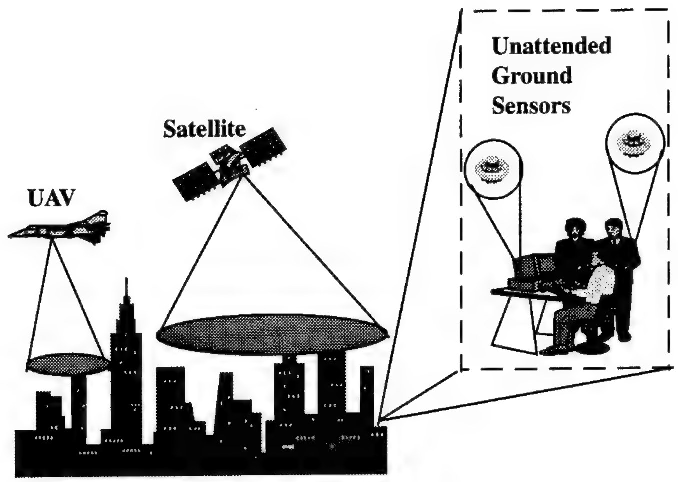
As mentioned previously, the AI system requires a cumulative database to help decision makers determine the possible LOVs of an adversary.[4] A portion of that AI database originates from the target acquisition system. Target acquisition involves the continuous collection of data for analysis and use by the AI network. A collection of sensors search for different types of signatures common to LOVs. This data is transmitted in virtual real time to the AI database to be analyzed and applied to the strategic attack process.

The target acquisition system does not simply push data to the AI network; it also must pull information from the network. Pulling information from the AI network narrows the search pattern for the sensor platforms and reduces the time required to locate specific targets. For example, the AI network may determine that an LOV for a certain adversary involves the capability to produce and employ chemical weapons. The target acquisition system can orient itself to search more efficiently by pulling from the AI network details such as the probable chemical composition and size of strategic production facilities about the LOV. Once the LOV is located, the sensor platforms periodically revisit the region to detect any changes in activity.

In order to locate specific LOVs, the target acquisition system requires novel sensors that essentially can see, hear, smell, taste, and touch. Current target acquisition systems for strategic attack depend heavily on sensors that only provide image data from the infrared and visual spectrums. Having different types of sensors in 2025 provides complementary data for the AI network to analyze and helps detect an adversary's LOVs.

The platforms supporting the sensor array vary, depending on the sensor's capability. As shown in figure 2-1, space and airborne platforms, including stealthy unmanned aerial vehicles (UAV), can operate jointly to provide the AI network continuous coverage of a specific region or land mass. Unattended ground sensors (UGS) rely on their minute size to avoid detection by an adversary. In 2025, sensors the diameter of a human hair will allow continuous, stealthy, on-site collection, providing the AI network the critical data necessary for making decisions concerning strategic attack.[5]

The final requirement for target acquisition in 2025 involves the necessity for sensor data to be transmitted instantaneously to the AI database. Sensor platforms such as satellites and UAVs can transmit data directly to relay stations on the ground or in orbit. Tiny unattended ground sensors depend on an external source to amplify sensor signals. The end result is complementary data from different sensor arrays delivered simultaneously to the AI network for analysis and application in the strategic attack process.




**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 2-1. Sensor Platforms**

## Target Engagement

In 1943, according to McKitrick and others in *The Revolution in Military Affairs*, the US Eighth Air Force prosecuted only 50 strategic targets during the entire year. In comparison, during the first 24 hours of Desert Storm, the combined air forces prosecuted 150 strategic targets—a thousand-fold increase over 1943 capabilities.[6]

In the year 2025, airpower and space power must make a similar leap in capability to ensure that the US maintains the advantage against its potential enemies. This will be accomplished through capabilities that affect LOVs in a very diverse manner. The system analysis and target acquisition processes provide the details of how to engage each LOV. These details can be characterized by the three boundaries depicted in figure 2-2. The first boundary ranges from lethal to nonlethal force. The second boundary involves the use of either direct or indirect means. The last boundary indicates that the time to engage an LOV will range from immediately to never.

The application of airpower has traditionally been accomplished by directly applying lethal force. However, many cases in the future will call for nonlethal force, especially when engaging another advanced "post-industrial" society. For example, against a third wave adversary we might attempt to disrupt, dominate, and then reorder an enemy's decision cycle.[7]

Although the Gulf War demonstrated that airpower can deliver direct, lethal force against a target set, there remains much room for improvement. As military force structures continue to downsize, we will lean towards systems capable of affecting multiple LOVs per mission. Instead of an F-117 flying over Baghdad to drop two precision guided munitions (PGM), it is more cost-effective to deliver dozens of PGM-type munitions on the same mission. In 2025, this capability allows a single mission to have the same results as a squadron of F-117s.

An organic, multiple engagement capability increases the application of air and space power throughout the enemy's strategic system with such great speed and momentum that hyperwar results. The simultaneous engagement of LOVs makes an adversary's recovery difficult because the remaining energy available to the system is inadequate to restore it to full capacity.[8]

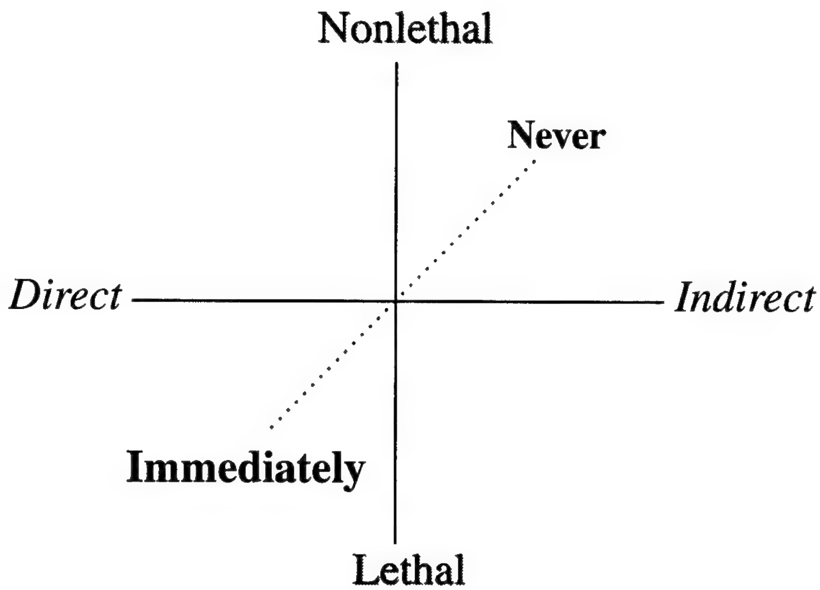



**Figure 2-2. LOV Engagement Spectrum**

The time to engage a strategic LOV can range from "immediate" to "never." An example of "never" is making a conscious decision not to attack an enemy's head of state, as in the case of Iraq's Saddam Hussein. Another example is the "Ultra" intercepts of Nazi war plans during World War II. Indeed, Churchill had to make numerous painful decisions not to defend Allied assets he knew were going to be attacked for fear of alerting the Germans to prior Allied knowledge of their plans.[9] On the other hand, we need the capability to engage some LOVs "immediately." An example is a convoy of nuclear, biological, and chemical (NBC) weapons discovered less than a mile away from a hardened storage facility deep inside a mountain. The US might have less than one minute to react and destroy these weapons before the engagement opportunity disappears.

The key to successful target engagement is having the air and space power to execute target engagements in terms of lethal or nonlethal force, direct or indirect means, and at the correct time. This will be accomplished by a combination of improvements in weapons and strategic attack platforms.

## Feedback

Following a target engagement, the AI network requires near-real-time postattack data to determine subsequent courses of action. Having an instant feedback capability shortens the operational timeline required for strategic attack in 2025. The same sensors used for target acquisition provide the necessary feedback data to the AI network. The data from different sensors is collected and then quickly fused into accurate mission evaluation results by the AI network. This feedback process answers the question as to the outcome of the strategic attack: To what degree did the mission succeed or fail, and did any positive or negative side effects occur that require further action?[10]

## Notes

1. Col Phillip Meilinger, *10 Propositions Regarding Air Power* (Air Force History and Museums Program, 1995), 1.

2. USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 25.

3. Ibid., 38–44.

4. The proposed system is designed provide suggested LOVs to human decision makers, along with the thought processes behind their selection. The human will then make engagement decisions.

5. Gary Stix, "Micron Machinations," *Scientific American*, November 1992, 107.

6. Jeffrey McKitrick et al., "The Revolution in Military Affairs," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future* (Maxwell AFB, Ala.: Air University Press, 1995), 78.

7. Barry R. Schneider and Lawrence E. Grinter, *Battlefield of the Future* (Maxwell AFB, Ala.: Air University Press, 1995), 149.

8. Col Richard Szafranski, "Parallel War and Hyperwar: Is Every Want a Weakness," in Barry R. Schneider and Lawrence E. Grinter, eds., *Battlefield of the Future* (Maxwell AFB, Ala.: Air University Press, 1995), 128.

9. Schneider and Grinter, 150.

10. The measure of success that the system would be reporting to human decision makers would focus on the desired effect on enemy decision makers.

## Chapter 3

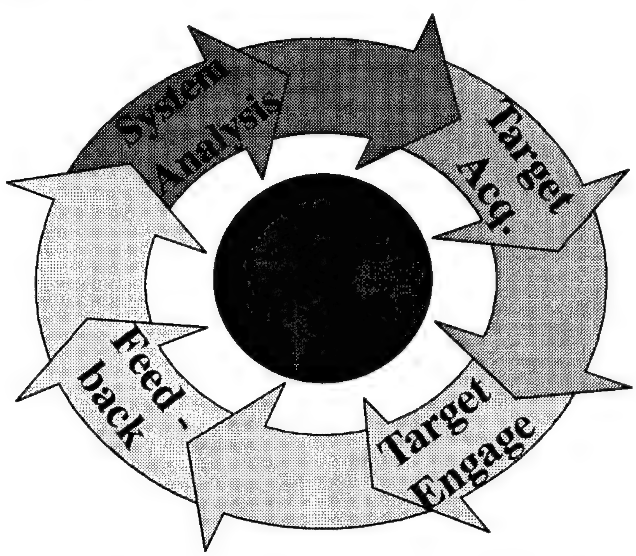
# Strategic Attack Systems Description

The process required to conduct strategic attack in 2025 uses a "system of systems," with each subsystem solving one particular part of the attack problem (fig. 3-1). The process is organic, in the sense that all of the parts are interlinked and interactive, each receiving and delivering input to the others. It provides targeting information containing the LOVs upon which the US should act, whether they are hard or soft, should be acted on now or never, lethally or nonlethally, and directly or indirectly.

### System Analysis System

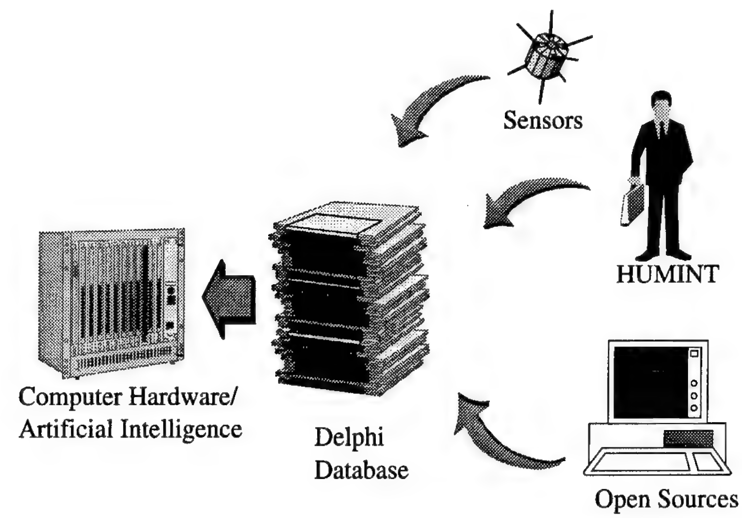
A component of the strategic attack model is the system analysis system, which will operate for decision makers in 2025. It will be composed of a pervasive, distributed, relational database; a blackboard artificial intelligence architecture; and a massively parallel, distributed computing capability. The system analysis system, shown in figure 3-2, functions to provide the decision makers with the knowledge that they need to direct strategic attack.

The ***2025*** system analysis system relies on a pervasive, distributed, and relational database.[1] The data comes from all sources, spanning the spectrum from state-of-the-art sensors collecting information in virtual real time, to archives on ancient history and culture. Because the database is so pervasive and distributed, it functions as a database of databases, with the primary users of each segment maintaining their separate parts. Its decentralized and partitioned structure permits data to be added or altered as future experience shows is necessary.[2] A depiction of this type of database arrangement is shown in figure 3-3. In this diagram, four widely separated databases combine to form the Delphi database for the strategic problem or problems that the system is working. The




**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 3-1. Strategic Attack Process**

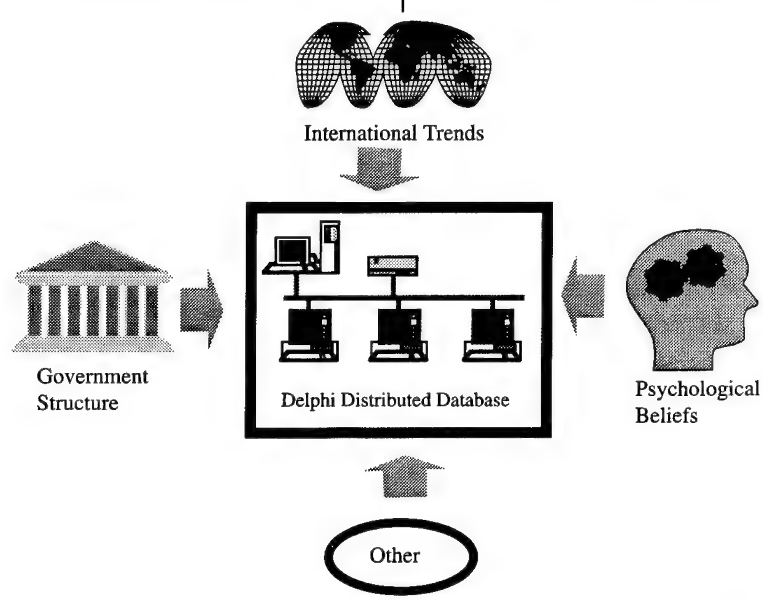



**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 3-2. The System Analysis System**

actual titles of the databases in figure 3-3 are notional. The important points to note are that the individual databases originate from virtually anywhere and are tied together by a network to comprise the Delphi system for solving a particular problem. A different set of variables would result in a different database combination.

The technology to facilitate this database will develop at varying rates, so the structure of the database allows the components to be incorporated as they emerge. Electronic data storage and access rates are advancing at a great pace. A recent study suggests that likely advances in optical disk technology and applications of




**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 3-3. Delphi Database**

"parallelism" hold the potential for significant increases in storage capacity.[3] Broadband fiber optic networking technologies that allow for the distributed nature of the system are advancing and will continue to improve volume and speed of data transfer. The USAF SAB postulates that ultra-high-speed broadband commercial backbone networks will be widely available by 2005. This infrastructure essentially gives infinite bandwidth to all users, therefore minimizing networks as a limiting factor for the database system.[4]

Access to diverse amounts of information could be a problem. As the value of information grows in the world economy, many distributed databases may become proprietary, denying the Department of Defense (DOD) access. The networked and distributed nature of the Delphi database requires the ability to secure the sensitive parts of it.

The Delphi database could, of course, be countered in a number of ways. The potential opponents of the US could shield the data that we desire. They could prevent our sensors from observing sensitive physical targets, or they could attempt to camouflage or obscure them. Opponents could close their societies, preventing us from collecting information concerning who their leaders are and how they think. Additionally, they could physically attack the data storage or transmission infrastructure or corrupt the data contained in the system. The best counter for attempts to prevent our data collection is a redundant and complementary collection system—many different types of sources. Possible countermeasures against data corruption include comprehensive physical security and defensive information warfare measures.

### Artificial Intelligence

AI involves programming a computer to solve problems that normally only people can handle. In 2025 AI provides the help that humans need to make strategic attack decisions. The role of AI is to constantly process the data stored in, and streaming through, the Delphi database. The ultimate goal is to use AI to determine the best way for the US to conduct strategic attack against an emerging opponent. A number of different AI approaches exist, a partial list of them includes expert systems, case-based reasoning (CBR), and neural networks (NN).

Expert systems turn the knowledge of a human expert into a computer program, and through an "if . . . then . . . else" process, applies that codified knowledge to similar, future problems. They cannot extend that knowledge outside the expert's field.[5] CBR is a technique that suggests actions by recognizing similarities between current problems and previously solved occurrences. Because CBR focuses on past problem resolutions rather than the current problem, it is quickly and easily implemented. To the point that new problems differ from those of the past, however, CBR has less value.[6] The third AI approach involves NN. They employ real-world ambiguous data points to determine a relationship, apply the relationship to make decisions, and constantly review the derived relationship to learn and improve the decision making process. Neural networks require, neither a human expert's knowledge nor past occurrences of the problem in order to function. Further, they can make constantly improving predictive decisions.[7]

The architecture of the AI portion of the system analysis process involves a modified blackboard expert as shown in figure 3-4. A blackboard system is a hybrid expert system comprised of a collection of independent components called "blackboard," "knowledge modules," and "control module."

The blackboard is the part of computer memory that contains the control module and the knowledge modules. The knowledge modules are a collection of independent components that, when combined, provide the information necessary to solve the problem. The modeler can choose the optimal AI technique for the problem being worked. Each knowledge module can function

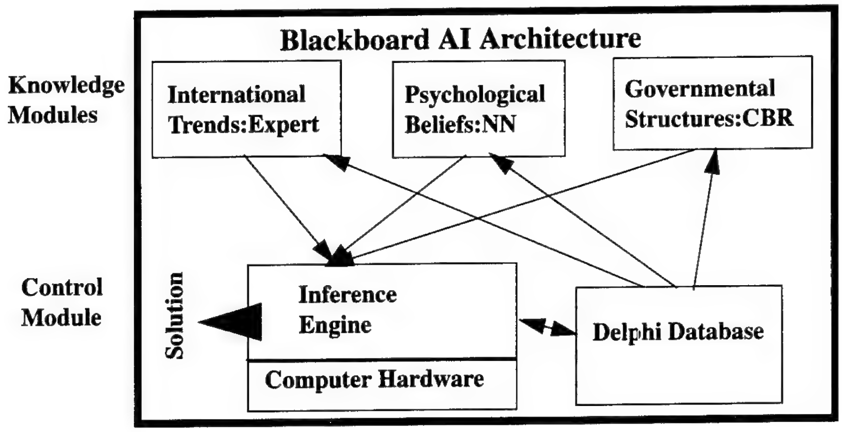



**Figure 3-4. Artificial Intelligence Architecture**

independently to determine an optimal solution for the problem that it is working.

The control module provides a vehicle for combining the outputs of the knowledge modules in order to arrive at a solution. It does this through the use of an "inference engine," an algorithm combining AI technologies. The control module considers all contributions from each knowledge module, selecting only those that are appropriate at the time. It weighs each contribution according to its value rating. The control module is linked to the Delphi database to monitor its operation, directing data to specific knowledge modules through the use of software agents.[8] By monitoring the database, the control module ensures that significant events get routed to the proper place in priority fashion. It devises workarounds and graceful degradation strategies if parts of it fail.

In figure 3-4, the control module combines an expert system, a CBR system, and a neural network system to make decisions. The presence of the first two ensures that the system has the knowledge necessary to make the right call. The use of the neural network adds the ability to learn from past events. A promising scheme for combining these different AI approaches is Fuzzy Approximation Theory, which weights the methods by variable amounts based on the traits of the adversary and the situation.[9]

The blackboard system also enables the proposed AI solution to be "what if'd." Before proposing a course of action (COA), the blackboard expert inputs the decision to a world database residing in memory and games the likely consequence. This simulation process is iterated until arriving at a COA that generates an optimal solution. The solution is then provided to the human decision maker. The "gaming" feature is essential in order to explicitly consider the interdependent nature of world affairs. In *New World Vistas*, experts assert that by 2020 the fuzzy methods required by the inference engine of the "control module" will mature and the ability to "game" proposed COAs will exist.[10]

Before an AI system can be reliably employed, much improvement is required. The techniques employed above have been used only at very basic levels. A university professor developed an expert system to explain US foreign policy decisions made in Asia. When his model was backcasted to the 1950s it predicted a very favorable 86 percent of the decisions that the US ultimately made.[11] CBR applications are being used commercially to handle customer service calls, with a technician

asking the customer questions that take him through a fault isolation tree developed from past product failures.[12] Many examples of neural networks are in operation today.[13] Finally, the Navy uses blackboard systems to manage complex electronic networks.[14] While these AI applications are simple compared to the requirements for 2025, they document the great strides being made in this field.

The AI portion of the system can be countered. AI requires the input of data to make decisions. If entered data is inaccurate or corrupted, the AI decisions will be degraded. Verifying the data and decisions for reasonableness minimizes this problem. Since the AI program operates in the electronic environment, it is subject to physical attack—either on the computers or on the electricity sources required to operate them. Steps to enhance the physical security of each major facility, combined with the distributed nature of the system, helps defend against these types of attacks. Finally, since AI is essentially a software-driven system, it is subject to information warfare attacks. This avenue of attack is best countered by an active counterinformation warfare capability.

### Computer Hardware Requirements

The significant capability of the system analysis system of 2025 depends on improvements in computing capability.[15] Current processors cannot run the AI programs this system requires.[16] However, massive parallel central processing unit (CPU), where a large number of processors are combined on individual silicon chips, are being exploited commercially today. Again, there remains room for much growth.[17] Technical experts maintain that the current exponential growth in computing performance based on silicon technology will continue through 2006, at which point material constraint will force alternate methods. Promising alternate technologies include quantum, molecular, and optical computing methods.[18]

## Target Acquisition System

In 2025, an organic relationship exists between target acquisition and the Delphi database. It is the classic "chicken or egg" relationship: the Delphi database must know the LOV exists before telling target acquisition sensors to find it; but the existence of the LOV may be discovered only after the target acquisition sensors collect initial data hinting at the LOV's existence. By necessity, therefore, the target acquisition phase operates continuously, passing streams of data to the Delphi database for analysis, while at the same time pulling fused information from the database to help guide the acquisition process.

The target acquisition system must provide decision makers the capability to detect changes in the personal values of an adversary. Changes in a leader's emotions, thoughts, or frame of reference are of interest to the strategic attack system. Techniques that get into the "head" of an adversary to obtain valuable information require revolutionary advances. Finding plausible methods for accomplishing this task is the focus of the classified "Information Attack" white paper. The target acquisition portion of strategic attack in 2025 complements these techniques with a diverse arsenal of sensor platforms.

Data collected by target acquisition sensors can range from single bits of data, like an LOV's exact location, to an entire library of data, such as the LOV's normal activity levels. In the year 2025, sensor collection provides enough data for a virtual 3-D model of the LOV to include its composition, internal structure, baseline characteristics, and tendencies. Using a biological warfare (BW) storage facility as an example, and in the most optimistic case, sensors determine the building's exact dimensions and floor plan. They then highlight possible soft spots. Sensors distinguish between rooms containing biological agents, test equipment, sleeping quarters, and even the snack bar.

Target acquisition sensors also construct a baseline, or living archive, of data concerning

routine activity and environmental conditions. Examples include the average number of people who enter and exit each day, the number of vehicles in the parking lot, and the level of noise generated by the facility. This baseline data, combined with 3-D modeling, provides benchmarks for detecting changes in data collection; for example, a sudden increase in vehicular traffic or human activity.[19] Changes in an LOV's baseline activity data can be flagged to determine its significance. The AI system, or a human imagery analyst, can determine if the LOV requires a closer look by target acquisition sensors.

### Target Acquisition Platforms

Target acquisition platforms in 2025 can be airborne, space-based, or ground-based. Function, cost, and vulnerability determine where to mount a sensor. It makes little sense to build expensive space platforms for sensors that work effectively from the ground.[20] On the other hand, some sensors may work effectively only above a certain altitude or from space. In any case, having a variety of platform types decreases an adversary's opportunity to completely stop sensor data collection and its transmission to the Delphi database.

A combination of commercial and military satellites should provide continuous worldwide coverage in 2025. Spatial resolutions of 10 meters, improved to two or three meters through signal-to-noise ratio calculations, will be available instantly and continuously.[21] In addition, expect multispectral, hyperspectral, and synthetic aperture radar images to provide periodic submeter resolution throughout a 24-hour span.[22] However, to obtain higher resolution images of LOVs on a *continuous* basis, airborne platforms must be employed.

Airborne sensor platforms can be described as standoff systems or overhead systems. A standoff system loitering along a political border at 50,000 feet can stare 230 miles downrange at an LOV and provide continuous one-meter resolution.[23] Unmanned aerial vehicles or simple high-altitude balloons could carry these sensors. In addition, a low-observable UAV that loiters directly over a specific area will carry sensors that provide continuous one-centimeter resolution.[24] The final type of sensor platform provides acquisition information that is unavailable from space-based assets.

Ground-based platforms in 2025 rely heavily on micromechanics and nanotechnology to shrink sensors and platforms to microscopic sizes.[25] These platforms could be inserted via human agents, through water or food supplies, or through aerial seeding operations using UAVs. Microsensors thinner than human hairs could transmit data to the Delphi database via UAV or satellite relay.[26] A swarm of ground-based microsensors could ensure constant data transmission of local conditions and activity levels near and inside an LOV.[27]

Except for micromechanical platforms, the *hardware* for most sensor platforms exists today. However, it is the sensors and not the platforms that collect the data to acquire the LOV. Therefore, the key to effective target acquisition in 2025 will be the development of critical sensor technologies. These technologies allow continuous collection of daytime, nighttime, and weather data that feeds the Delphi database to generate new LOVs.

### Critical Target Acquisition Sensor Technologies

Successful target acquisition depends on critical sensor capabilities that will require much more development before the year 2025. To simplify their descriptions, the sensors can be compared to the human ability to see, hear, smell, and taste. And just like in humans, the sensor data collected can be fused by the Delphi database to provide accurate information concerning LOVs. Traditionally, the "seeing" technologies dominated the sensor field using spectral analysis of the visual and infrared (IR) bands, along with SAR returns.[28]

In 2025, radically different sensors add critical data to confirm or dispute what we think we "see." Having sensors that provide complementary data (instead of duplicating data) ensures better accuracy and reliability. It also prevents an enemy from defeating the entire system by destroying, or defending against, one type of sensor.[29]

**Visual Sensors**. Multispectral Imaging (MSI) currently dominates the sensor field. As mentioned before, the use of the visual and IR bands, plus synthetic aperture radar (SAR) can provide resolution from 10 meters to one centimeter, depending on the platform distance from the LOV and loiter capability.[30] New technologies, like hyperspectral imaging, laser-light detection and ranging, and magnetic resonance imaging, can provide other methods to paint an LOV.

Instead of concentrating on a single broad-spectrum band, hyperspectral imaging involves slicing the entire electromagnetic spectrum into hundreds or thousands of single-wavelength data bands for collection.[31] The bands that produce a signature can be fused together by the Delphi database to construct a target signature.[32] LOVs may be able to avoid detection in one spectrum but not from all spectrums.[33] Due to size and weight, hyperspectral sensors will likely require airborne or space-based platforms.

Laser-based light detection and ranging (LIDAR) sensors offer great hope for detecting atmospheric changes due to chemical and biological reactions. By actively probing the atmosphere, LIDAR sensors will detect and construct 3-D images of aerosol clouds common to factories and machines. One can develop a best guess as to what a factory or machine produces by comparing predetermined aerosol images of known substances.[34] These sensors could also be used to warn of possible chemical and biological warfare agents on a battlefield. Future LIDAR sensors will easily fit in a small suitcase, making them adaptable for satellite and UAV platforms.[35]

Magnetic resonance imaging (MRI) is a sensor technology that is useful in building 3-D images of LOVs in 2025. An MRI sensor offers the advantage of imaging the internal, as well as external, structure of the LOV. UAVs could blanket a building with specially designed dust particles that circulate throughout the structure's ventilation system.[36] Then MRI equipment and sensors carried on space-based or airborne platforms could scan the structure, analyzing the circulation of the dust particles to construct an internal image of the LOV.

**Sound Sensors**. Sound sensors can measure vibrations in the atmosphere or through materials. The ability to listen to human conversations using microphones mounted on space platforms may be available in 2025, but it will be expensive. A cheaper method involves miniature microphones built through micromachining. These sensors, the size of pinheads, could be planted via UAV seeding operations, human agents, or even letters sent through the mail.[37] The ability to listen to an LOV and its surrounding environment will provide early warning of an adversary's intention, especially when fused with the cues detected by visual sensors.

A second use for acoustical microsensors involves measuring seismic vibrations and mechanical resonance. Acoustic resonance spectroscopy can reveal the contents of sealed containers by analyzing the container's mechanical resonance.[38] Using a horde of tiny microphones, an entire structure could be analyzed and the data from each sensor relayed to the Delphi database via an overhead collector. These sensors could also be used for seismic mapping of underground facilities (like command bunkers) that escape detection by visual sensors.[39]

**Smelling Sensors**. In 2025, olfactory sensors will be similar in size to microscopic hearing sensors. Unlike the LIDAR system that detects signatures of aerosol clouds, smelling sensors can detect the actual chemicals themselves. Organic thin film coatings on tiny platforms will contain prefabricated "molecule buckets" to trap suspected chemical molecules. If the chemical is present, the buckets fill up, changing the

organic property of the platform.[40] When irradiated by ultraviolet or X-ray energy, these organic changes can be scanned and analyzed by overhead sensors.[41]

Another novel smelling technology available in 2025 involves tracking humans via genetically linked body odors.[42] These odors, undetectable by the human nose, can be sensed by bundles of sensors that then transmit the data to the neural network portion of the Delphi database. Since each sensor reacts differently to chemical compounds, specific compounds can be identified.[43] If it is possible to get an "odor" sample of an enemy leader, then olfactory sensors could be used to detect and track the human LOV.

**Tasting Sensors**. Sensors that transmit data after tasting an LOV can provide discriminating clues for the Delphi database in 2025. Tasting sensors can be prefabricated to detect—and attach to—certain types of surfaces, similar to the way smelling sensors have prefabricated molecule buckets. A variety of tiny taste sensors could be dispersed over an LOV, and then irradiated and scanned to gather data.[44] Taste sensors designed to detect aluminum would stick to aluminum aircraft wings but fall off wooden decoys. Other sensors could taste buildings or vehicles for radioactive fallout, chemical residues, or biological agents.[45]

If sensors can be designed to attach to specific compounds in 2025, they can be designed to attach to specific people. Like prickly cockleburs, tiny sensors would cling to certain humans, effectively tagging them for continuous tracking via overhead platforms.[46] If a human LOV cannot be tagged specifically, certain items common to that person, like vehicles and clothing, could be tagged for tracking. Possessing the ability to detect and track a human LOV adds greater flexibility to the strategic attack process.

A constellation of sensors provide the tools for detecting and tracking LOVs in 2025. These sensors form the backbone of the target acquisition phase, offering overlapping and complementary capabilities. The data collected is delivered to the Delphi database, where LOVs can be determined and courses of action formulated. When a decision is made to commence strategic attack, the target engagement platforms receive whatever information has already been collected. That information will include the LOV's description, location, weaknesses, strengths, and the suggested method of attack to achieve the desired effect.

## Target Engagement System

The third component of the strategic attack process is target engagement. It provides the method for generating strategic effects in 2025. The targets identified for strategic attack vary widely based on the adversary and the situation, and require a diverse arsenal of capability. This arsenal must include means to affect hard and soft LOVs directly or indirectly, using lethal or nonlethal power, and within an immediate to indefinite time frame. Futuristic engagement systems and techniques such as holographic projection, noise and gravity fields, biomedical operations, psychological operations, military deception, and information attack are all possible. These innovative indirect means are discussed in the classified $C^2$ and Information Attack white papers. As a complement to those indirect techniques, this paper focuses on target engagements that use direct attacks with lethal and nonlethal power.

In 2025, the effectiveness of an attack is a critical factor. In the *New World Vistas Summary Volume*, modeling experts showed that "if the effectiveness of the attacker is increased from one to five, and the initial forces are equal in number, the attacker will lose approximately 10 percent of the force while destroying the enemy entirely."[47] Since the ***2025*** Alternate Future study depicts a smaller US military in most cases, we need to significantly increase our attack effectiveness through improvements in weapons and delivery platforms.[48]

**Weapons**

By 2025, conventional explosive weapons will be more accurate and their explosive effectiveness per unit mass will be higher by a factor of 10 than those of today.[49] The miniaturized munitions technology demonstration's (MMTD) goal is to produce a 250-pound munition that is effective against a majority of hardened targets previously vulnerable to only 2,000-pound munitions. A differential global positioning system/inertial navigation system (GPS/INS) system will be an integral component of the MMTD to provide precision guidance. These guidance and smart fusing techniques will produce a high probability of target kill.[50] Self-targeting missiles will compliment the MMTD. These missiles have microoptics, aerodynamic actuator arrays, active skins, and microelectromechanical system (MEMS) technologies. The many advantages of these missiles include standoff capability and relatively cheap production costs.[51] Conventional weapons, however, will not provide the full range of options required in 2025.

Although many of the weapons used today will still be employed in 2025, directed energy weapons (DEW) have great potential for strategic attack missions. The three general classes of DEWs are laser, radio frequency (RF), and energetic particle beam. They present an excellent complement to conventional weapons due to their characteristics. First, some DEWs have a higher probability of hit compared to projectiles. This is because the spreading beam can irradiate the entire target, therefore requiring less pointing and tracking accuracy. Second, they offer near-instantaneous engagement capability in most weather conditions. Third, each has a large magazine compared with the typical aircraft store of conventional projectiles and missiles.[52] Fourth, DEWs have the potential to be much cheaper to support than conventional explosives. The traditional bomb loading, fusing, and storage facility could be replaced by the "fuel" required to source the DEW. Last, and maybe most important, DEWs can be nonlethal in some applications.

Lasers will be the first to become operational on our strategic attack platforms. Significant progress has already been made in the airborne laser (ABL) program, under way since 1992. The program gives the US military a credible boost-phase defense against theater ballistic missiles. This laser is slated to be flight-tested in 2002 and fielded in 2006. Each laser shot is estimated to cost only $1,000 in "laser fuel," which is a mixture of common chemicals.[53] Cost-effectiveness is further enhanced by a single mission being able to deliver multiple shots prior to mission completion. Recent success in using high density polyethylene (HDPE) plastic in the chemical oxygen iodine laser (COIL) can save on material cost by a factor of 100 and on machining cost by a factor of three—all without degrading laser performance. Because it is nine times lighter than the metals normally used in constructing lasers, HDPE is an ideal choice for an airborne COIL platform.[54] Through techniques like these, we can make lasers small and light enough to become modular weapons systems on our strike platforms. Limitations of lasers include being fair-weather weapons and requiring dwell times in the range of seconds; however, RF weapons can be used to compensate for these weaknesses.

The RF weapon showing the most promise is the high power microwave (HPM). It is not limited by weather and requires less than a second of dwell time on a target. The HPM's effect on electronic devices ranges from disruption to destruction, depending on the target's electromagnetic susceptibility and the HPM parameters. Energy from an HPM weapon can couple into system electronics through front door or back door paths at frequencies that may be either in-band or out-of-band. This means that electronics can be burned out even when the system is turned off.[55] In general, the susceptibility of electronics to an HPM increases as the scale size of the

electronics decreases, making the most modern electronic systems potentially the most vulnerable.[56]

High power microwave weapons also provide great flexibility in their lethality by having "dial-a-frequency" options. In most cases, the HPM could be targeted against electronic systems and be tuned to a frequency that would pass harmlessly through humans. On the other hand, if the situation required, the HPM could be used against enemy personnel. It could be set at a low power to cause sufficient pain to stop enemy personnel, or "turned up" to actually burn troops to death.[57]

Both laser and HPM weapons have the added benefit of providing our platforms organic self-protection capability. Just as the ABL can engage theater ballistic missiles, our strike platforms could use their organic DEW weapons to destroy attacking missiles. The laser would require a direct hit, while the HPM weapon could be less accurate and still have the same positive results. The HPM approach also has the potential of being a "force shield" for the strike platform if engaged by multiple threats simultaneously.[58] The major disadvantage of HPM is the danger of fratricide, since US systems rely so heavily on electronics. Safeguards and procedures must be integrated in the weapon system to prevent this hazard.

Energetic particle beams offer the most potent form of DEW, since their penetrating power is robust against the most stringent hardening measures.[59] As an analogy, using lasers and HPMs is like shooting BBs at a target while the particle beam is like firing baseballs. Unfortunately, the atmosphere significantly degrades the particle beam's propagation over long ranges and limits its usefulness on earth. Since similar atmospheric propagation problems do not exist in space, and MEMS developments will shrink the size of these weapons appreciably, it is likely that energetic particle beams can be used to conduct strategic attacks against enemy LOVs in space.

**Strategic Platforms**

Strategic attack platforms will involve UAVs, transatmospheric vehicles (TAV), and space-based systems. UAVs will be prevalent in the future, and many of them will support the strategic attack mission. Their benefits and specifications are detailed in the ***2025*** UAV white paper. Because the UAV has a slow response time, newer platforms like the TAV and space-based systems are required. TAVs and space-based platforms can satisfy the portion of strategic attack in 2025 that requires immediate and massive firepower to accomplish great shock value.

The ***2025*** "Spacelift" and "Through the Looking Glass" white papers provide the specifications of a plausible force application TAV and space-based weapons. However, many of their characteristics are restated in this paper because they directly support the strategic attack mission. The TAV would be capable—from an alert posture—of arriving at a target anywhere in the world within one hour of notification. Its weapons bay would be modular to allow several different types of weapons for increased flexibility. TAVs returning from a mission could be serviced and ready to fly again in less than a day, and could be surged to fly multiple missions per day if necessary.

The TAV platform capitalizes on several principles of war. It is offensive, bringing the fight to the enemy on our terms. The TAV provides surprise, striking enemy targets at any depth with little or no warning. Additionally, it delivers massed effects by employing precise firepower. Just as the F-117 carrying PGMs delivered on the principles of mass and economy of force during the Gulf War, the TAV will take this one step further. This platform accomplishes multiple attacks over a diverse target set during a single mission. Ultimately, with the appropriate weapons load, it can engage targets in separate major regional contingencies during a single mission (fig. 3-5). In short, the TAV provides a timely threat to strategic targets anywhere on the globe.

The vehicle must be designed to incorporate a modular weapons system. This concept increases cost effectiveness by allowing the TAV to be used for a variety of military missions, from force enhancement through force application. These weapon modules are maintained in readiness, stored until needed, and then quickly loaded on the vehicle. Finally, better sustainability can result from quick reloads and rapid turn-times. The TAV will provide quick reaction time across the globe; however, some cases will require more immediate strategic attack.

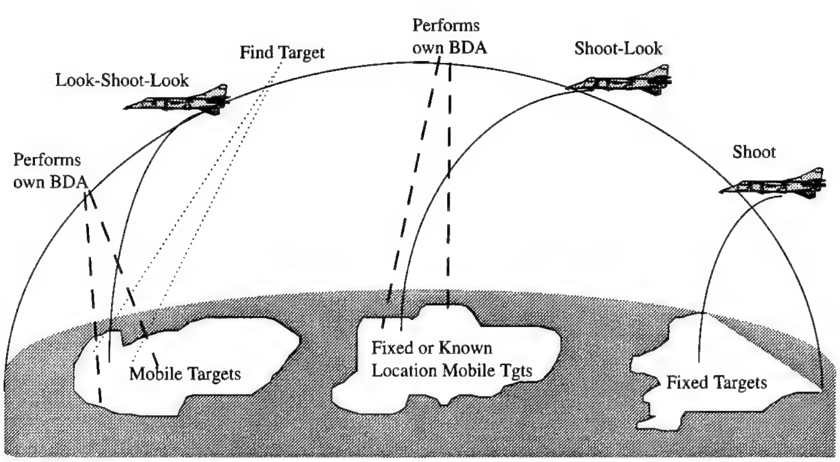
Utilizing a space-based platform is a powerful strategic attack option because it truly provides an "anytime . . . anywhere" engagement capability. Two generic deployment strategies exist. The first is an autonomous weapon deployed in space along with beam directing optics and control systems. This approach creates significant problems due to space logistics, resupply, targeting, and control. Additionally, it raises political issues related to the placement of offensive power in space. These technological difficulties and political issues make a second deployment option more attractive.[60]

Constructing a DEW on the ground and deploying targeting mirrors in space is the more feasible option. Having the source of energy on the ground means that laser energy will not be limited by satellite power or by available fuel. The large targeting mirrors, built with lightweight structures, could employ wave front compensation to correct for optical imperfections.[61] These spaced-based mirrors provide the capability to immediately apply lethal and nonlethal DEWs on a strategic LOV.

## Feedback Systems

The last ingredient of the organic strategic attack process is feedback. Feedback provides the Delphi database with a near-instant awareness of an LOV's status. It answers the question as to the outcome of the strategic attack: Did the mission achieve success, failure, somewhere in between, or overkill? Knowing how much or how little an LOV was affected allows the system analysis network to generate subsequent courses of action.

Traditionally, feedback in the strategic attack process has been called battle damage assessment (BDA). In 2025, strategic attack may not involve "battle" with an enemy to




**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 3-5. Transatmospheric Vehicle**

inflict "damage" to its personnel and equipment. Nonetheless, the "assessment" part of BDA remains a constant requirement for efficient and effective strategic attack.

The platform and sensor capabilities required for feedback in strategic attack are the same as those discussed in the target acquisition phase. This further illustrates the organic nature of the strategic attack process as a whole. The visual sensors placed on space and airborne platforms can provide continuous multispectral images of LOVs. However the importance of visual sensors may decrease in 2025 as the strategic attack process relies more on nonlethal methods of attack. In this case, nontraditional sensors that can hear, smell, or taste become essential by providing important bits of data that allow the Delphi system to piece together the effectiveness of an attack.

## Notes

1. ***2025*** Concept, no. 900374, "Living World-Wide Intelligence Data Basing," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

2. Joseph W. Wilkinson, *Accounting Information Systems: Essential Concepts and Applications*, 2d ed. (New York: John Wiley & Sons, 1993), 219–21.

3. USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 87.

4. Ibid.

5. John W. Griesser, "Experts among Us," *Business Horizons* 35, no. 3 (May–June 1992): 77–80.

6. J.J. Daniels and E.L. Rissland, "A Case-Based Approach to Intelligent Information Retrieval," 1995. On-line Internet, 3 January 1996, available from http://cbr-www.cs.umass.edu/abstracts.html#Daniels:CBR-Approach-to-IR.

7. Peter J. Denning, "Neural Networks," *American Scientist* 86, no. 4 (July–August 1992): 426–29.

8. ***2025*** Concept, no. 900446, "Automated Enemy Analysis Software," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

9. Bart Kosco, *Fuzzy Thinking, The New Science of Fuzzy Logic* (New York: Hyperion, 1993), 156–223.

10. *New World Vistas*, summary volume, C1-C15. The study suggests that the best approach for using software agents in this fashion is to have the agent generate specific data/task requests, rather than have it remotely travel the distributed database.

11. Charles S. Taber, "POLI: An Expert System of U.S. Foreign Policy Belief Systems," *American Political Science Review* 86, no. 4 (December 1992): 888–904.

12. Daniels and Rissland.

13. Denning, 426–29.

14. Randall J. Calistri-Yeh, "Applying Blackboard Techniques to Real-Time Signal Processing and Multimedia Network Management," *Proceedings of the 7th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems* (Austin, Tex.: IEA/AIE, June 1994), 593–99.

15. ***2025*** Concept, no. 900397, "Multi-Concurrent Operations CPU," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

16. ***2025*** Concept, no. 900791, "Quantum Mechanical Computer," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

17. George Gilder, *Microcosm* (New York: Simon & Schuster, 1989), 319–30.

18. *New World Vistas*, summary volume, 90.

19. Oscar Firschein, "Defense Applications of Image Understanding," *IEEE Expert*, October 1995, 11–17.

20. *New World Vistas*, summary volume, 22.

21. Ibid., 21.

22. Ibid.

23. Ibid., 22

24. Ibid.

25. Gary Stix, "Micron Machinations," *Scientific American*, November 1992, 107.

26. Naomasa Nakajima, "Micromachines," *The Futurist*, January 1994, 50.

27. ***2025*** Concept, no. 900288, "Swarms of Micro-Machines," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

28. "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," *Airpower Journal* 9, no. 2 (Summer 1995): 14.

29. Ibid., 12.

30. *New World Vistas*, summary volume, 21.

31. ***2025*** Concept, no. 900215, "Weather Data Collection/Display," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

32. "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 15.

33. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the sensors volume, 15 December 1995), vi.

34. William B. Scott "LIDAR System to Detect Biological Warfare Agents," *Aviation Week & Space Technology* 143, no. 2 (13 November 1995): 44.

35. Michael Black, "Technology's Brightest Stars," *R&D Magazine: The International Magazine of Research and Development*, October 1993, 58.

36. "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 12.

37. David E. Newland, "Acoustic Micromachines," *Nature* 370, no. 6484 (7 July 1994): 21.

38. "Three DOE Devices Will Assist in Weapons Dismantlement," *R&D Magazine: The International Magazine of Research and Development*, September 1995, 36.

39. "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 17.

40. Barbara Smith, "Technology Takes the Pinch Out of 'Going Green'," *R&D Magazine: The International Magazine of Research and Development*, September 1995, 45.

41. "New World Vistas" (unpublished draft, the sensors volume), 164.

42. Clive Cookson, "The Rise of the Robot Nose," *World Press Review* 42, no. 9 (September 1995): 36.

43. Otis Port, "A Nasal Network to Sniff Out Friend or Foe," *Business Week: Industrial/Technology Edition*, no. 3454 (11 December 1995): 115.

44. "New World Vistas" (unpublished draft, the sensors volume), 164.

45. "Leveraging the Infosphere: Surveillance and Reconnaissance in 2020," 18.

46. ***2025*** Concept, no. 900469, "Hitchhiking Sensors," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

47. *New World Vistas*, summary volume, 7. The importance of this quote is as a point of contrast for the expanded engagement capabilities that attack platforms will need in 2025.

48. Maj John Geis et al., "Alternate Futures," briefing (Air War College, Maxwell AFB, Ala.: 13 February 1995).

49. *New World Vistas*, summary volume, 9.

50. Lt Col Ted O. Mundelein, "Miniaturized Munition Technology Demonstration" (Unpublished paper, Eglin AFB, Fla.: January 1996).

51. Terry Neighbor, "Wright Laboratory ***2025*** Technologies Air Power Day," ***2025*** Lecture (Air War College, Maxwell AFB, Ala.), 13 November 1995.

52. John T. Tatum, "A New Threat to Aircraft Survivability: Radio Frequency Directed Energy Weapons," *Aircraft Survivability*, Fall 1995, 11.

53. Steve Watkins, "Service Closes in on an Airborne Laser," *Air Force Times*, 21 August 1995, 25.

54. Phillips Laboratory Computational Services Division, "Plastic Fabrication of Chemical Oxygen Iodine Laser (COIL) Devices," Phillips Laboratory, on-line, Internet, 25 March 1996, available from http://www.plk.af.mil/SUCCESS/coil.html.

55. Dr William L. Baker, "Air Force High-Powered Microwave Technology Program," *Aircraft Survivability*, Fall 1995, 9.

56. Ibid.

57. Col William G. Heckathorn, "Advanced Weapons and Survivability Directorate Vision," ***2025*** Lecture, Air War College, Maxwell AFB, Ala.: 4 December 1995.

58. Baker, 9.

59. Dr Louis C. Marqet, "Aircraft Survivability and Directed Energy Weapons," *Aircraft Survivability*, Fall 1995, 7.

60. *New World Vistas*, summary volume, 47–48.

61. Ibid., 47.

## Chapter 4

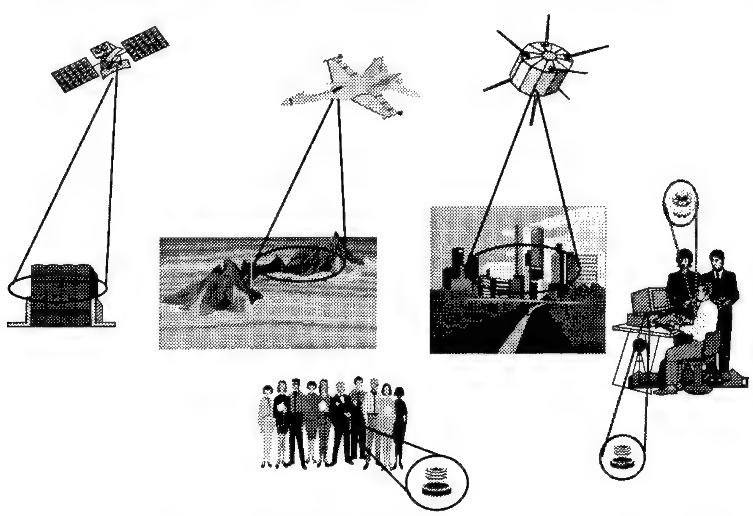
# Concept of Operations

The goal of strategic attack in 2025 is to conduct operations "to a point where the enemy no longer retains the ability or will to wage war or carry out aggressive activity."[1] Those operations run the gamut from traditional, highly destructive, force-on-force encounters to much less invasive, but very effective computer-based warfare. In 2025, advances in technology will improve the ability of the US to bring air and space power to bear on an adversary to achieve such war-winning effects. A description of the 2025 strategic attack system follows, based upon the technologies and organization outlined in the body of this paper. This system has four organically linked components: a system analysis system, a target acquisition system, a target engagement system, and a feedback system.

Data from all over the world, in virtually every form, is monitored by the system analysis system. This collection of databases, called the Delphi system, is managed by advanced AI technology. As world developments occur, the AI portion of the system determines which databases contain useful facts. The data originates from various military, commercial, and institutional sources. The Delphi system analyzes this data and determines solutions to the strategic problem in terms of what LOV to target and how to affect it. It feeds that information to human decision makers and the target acquisition system.

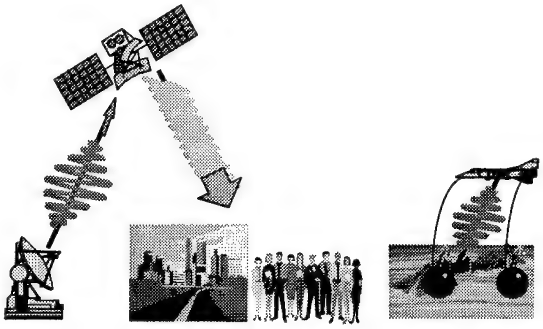
The target acquisition system in figure 4-1 uses sophisticated visual imaging and acoustical sensors to collect data from airborne platforms. It also employs ground-based microsensors to gather additional facts. It updates the Delphi database by providing LOV characteristics, such as location and composition, and makes this information available to the target engagement system.

Once national authorities decide to implement the recommendations provided by the Delphi system, the target engagement system depicted in figure 4-2 is employed. The engagement system encompasses a



**Source:** Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 4-1. Notional Target Acquisition System**



Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

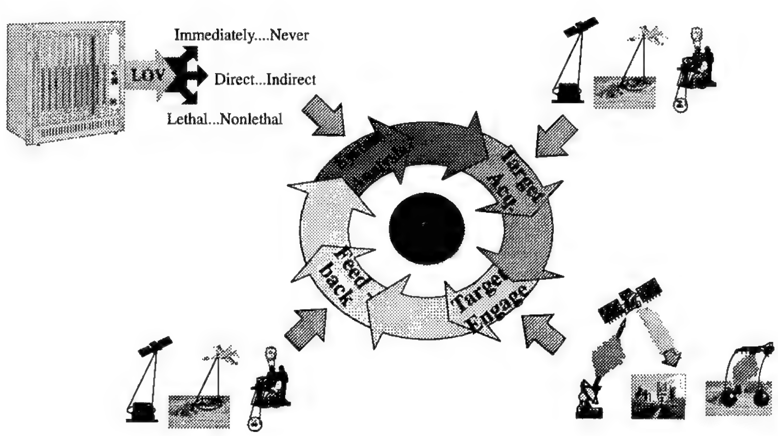
**Figure 4-2. Notional Target Engagement System**

broad range of tools to conduct psychological operations, perform computer-based attacks, deliver powerful conventional weapons from TAVs and UAVs, and utilize DEWs from space. This paper concentrated on attacking physical LOVs; however, as mentioned earlier, strategic effects can come from many approaches. This physical attack focus is intended to complement other ***2025*** white papers that detail innovative approaches for affecting less tangible LOVs.

The targeting system queries the Delphi database for the information necessary for engagement. The database delivers this product after updating relevant information by communicating with the sensor arrays feeding the acquisition system. Based on the desired effect, the targeting system selects the proper platform and weapon for the LOV. During and after the attack, the acquisition system monitors the target and reports its status to the Delphi system. Delphi uses its AI component to determine the degree of target engagement effectiveness. Delphi then reports that information to national leaders, along with the next recommended course of action. The outcome is a series of precise attacks with effects across the depth and breadth of an adversary. Figure 4-3 depicts the total strategic attack system.

**Note**

1. Department of the Air Force, Air Force Doctrine Document 1, "Air Force Basic Doctrine" (draft) (Langley AFB, Va.: USAF Doctrine Center, 15 August 1995), 13.




Source: Microsoft Clipart Gallery ©1995 with courtesy from Microsoft Corporation

**Figure 4-3. Strategic Attack in 2025**

# Chapter 5

# Investigative Recommendations

Examination of the required capabilities for a strategic attack system in 2025 revealed several high payoff technologies. Chief among the critical requirements are computing ability, artificial intelligence, nanotechnology, directed energy weapons, and transatmospheric vehicles.

At the foundation of the strategic attack system lies the continued improvement in computational and data storage ability. These two required capabilities are found throughout the organically connected subsystems of strategic attack. While critical, these technologies should not be the focus of military research and development efforts. The rapid, global growth of information-based societies recognize this as a lucrative area for private investment. Scarce DOD dollars should be spent elsewhere.

Sophisticated AI advances are necessary. AI applications and a branch of AI, intelligent software agents, are critical keys to building a Delphi system that provides decision makers with the information to make optimal decisions in 2025. The military will not be alone in its quest to advance AI; many segments of the commercial sector also plan to use it. Improved profit opportunities motivate industries to invest in this area. The task of military leaders and long-range planners is to determine what unique military applications exist in the field, and then selectively fund them.

Selective funding is also required to exploit the budding science of nanotechnology. This technology forms the baseline for some sensors and weapons that the strategic attack system requires. Microsensors used for tagging potential targets, or scattered to monitor specific areas, rely heavily upon nanotechnology. Further, this capability creates smaller weapons for use on UAVs or TAVs.

Another potentially high return area of technology concerns directed energy weapons. DEWs offer a flexible, timely, affordable means to affect an adversary's LOV. They can be "tuned" for a wide range of effects, from low-order intervention to high-order destruction. Additionally, the low cost of DEWs makes them cost-effective. Finally, the speed, ubiquity, and aura of power associated with DEWs provide significant flexibility in execution and have a profound deterrent value.

The TAV is yet another important enabling technology. The TAV retains the flexibility and on-the-fly innovation of manned vehicles. Further, the TAV's inherent speed allows for rapid engagement time. Finally, CONUS-based TAVs shrink the logistical tail, reduce security exposure, and create virtual global presence. The DOD should develop the TAV concurrently with the private spacelift industry.

# Chapter 6

# Conclusions

Strategic attack has always held a position of importance in the conduct of warfare. Done correctly, strategic attack shortens the fighting and reduces the costs. All warriors dream of conducting it with decisive effect, yet few have been successful. The difficulty usually centers on determining, locating, or engaging the correct LOV. This white paper identifies the most promising technologies and combines them to form an organic system for conducting strategic attack in 2025. Embracing these concepts provides a "hit 'em where it hurts" capability to successfully prosecute strategic attack.

# Bibliography


Baker, William L. "Air Force High-Powered Microwave Program." *Aircraft Survivability*, Fall 1995, 9.

Black, Michael. "Technology's Brightest Stars." *R&D Magazine: The International Magazine of Research and Development*, October 1993, 58.

Calistri-Yeh, Randall J. "Applying Blackboard Techniques to Real-Time Signal Processing and Multimedia Network Management." *Proceedings of the 7th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems*, June 1994, 593–599.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, N.J.: Princeton University Press, 1976.

Cookson, Clive. "The Rise of the Robot Nose." *World Press Review* 42, no. 9 (September 1995): 36.

Daniels, J.J. and Rissland, E.L. "A Case-Based Approach to Intelligent Information Retrieval." on-line, Internet, 3 January 1996, available from http://cbr-www.cs.umass.edu/abstracts.html#Daniels:CBR-Approach-to-IR.

Denning, Peter J. "Neural Networks." *American Scientist* 86, no. 4 (July–August 1992): 426–429.

Department of the Air Force. Air Force Doctrine Document 1. "Air Force Basic Doctrine" (draft). Langley AFB, Va.: USAF Doctrine Center, 15 August 1995.

Firschein, Oscar. "Defense Applications of Image Understanding." *IEEE Expert*, October 1995, 11–17.

Gilder, George. *Microcosm*. New York: Simon & Schuster, 1989.

Griesser, John W. "Experts among US." *Business Horizons* 35, no. 3 (May–June 1992): 77–80.

Grinter, Lawrence E., and Barry R. Schneider. *Battlefield of the Future*. Maxwell AFB, Ala.: Air University Press, 1995.

Kosco, Bart. *Fuzzy Thinking, The New Science of Fuzzy Logic*. New York: Hyperion, 1993.

"Leveraging the Infosphere: Surveillance and Reconnaissance in 2020." *Airpower Journal* 9, no. 2 (Summer 1995): 10–25.

Marqet, Louis C. "Aircraft Survivability and Directed Energy Weapons." *Aircraft Survivability*, Fall 1995, 7.

McKitrick, Jeffrey, et al. "The Revolution in Military Affairs." In *Battlefield of the Future*. Edited by Barry R. Schneider and Lawrence E. Grinter. Maxwell AFB, Ala.: Air University Press, 1995.

Meilinger, Col Phillip. *10 Propositions Regarding Air Power*. Air Force History and Museums Program, 1995.

Mundellein, Lt Col Ted O. *Miniaturized Munition Technology Demonstration*. Eglin AFB, Fla.: January 1996.

Nakajima, Naomasa. "Micromachines." *The Futurist*, January 1994, 50.

Newland, David E. "Acoustic Micromachines." *Nature* 370, no. 6484 (7 July 1994): 21–28.

Port, Otis. "A Nasal Network to Sniff Out Friend or Foe." *Business Week: Industrial/Technology Edition* 3454 (11 December 1995): 115.

Scott, William B. "LIDAR System to Detect Biological Warfare Agents." *Aviation Week & Space Technology* 143, no. 2 (13 November 1995): 44.

Smith, Barbara. "Technology Takes the Pinch Out of 'Going Green'." *R&D Magazine: The International Magazine of Research and Development*, September 1995, 45.

Stix, Gary. "Micron Machinations." *Scientific American*, November 1992.

Szafranski, Col Richard. "Parallel War and Hyperwar: Is Every Want a Weakness?" In *Battlefield of the Future*. Edited by Barry R. Schneider and Lawrence E. Grinter. Maxwell AFB, Ala.: Air University Press, 1995.

Tabor, Charles S. "POLI: An Expert System of US Foreign Policy Belief Systems." *American Political Science Review* 86, no. 4 (December 1992): 888–904.

Tatum, John T. "A New Threat to Aircraft Survivability: Radio Frequency Directed Energy Weapons." *Aircraft Survivability*, Fall 1995.

Toffler, Alvin and Heidi. *War and Anti-War*. New York: Little, Brown and Co., 1993.

***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

"Three DOE Devices Will Assist in Weapons Dismantlement." *R&D Magazine: The International Magazine of Research and Development*, September 1995, 36.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century*, Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

______. *New World Vistas: Air and Space Power for the 21st Century*, Sensors Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

Watkins, Steve. "Service Closes in on an Airborne Laser." *Air Force Times*, 21 August 1995, 7.

Wilkinson, Joseph W. *Accounting Information Systems: Essential Concepts and Applications*. 2d ed. New York: John Wiley & Sons, 1993.

# Close Air Support (CAS) in 2025: "Computer, Lead's in Hot"

Comdr Ronald J. Unterreiner (USN)
Maj Richard J. Findlay (USMC)
Maj Jeffrey A. Brelsford
Maj John F. Hunnell
Maj Michael F. Wagner

## Executive Summary

The mission of close air support (CAS) currently exists in every service doctrine and will continue to be required in 2025. Advances in technology will reduce the many shortfalls currently causing concern regarding the CAS mission. In 2025, time-critical applications of airpower and space power in support of troops on the ground will be vastly simplified from the perspective of both the tasker and the attacker. This paper describes the requisite systems and technology needed for aircraft to perform the mission. It does not discuss organizational issues.

Advances in ground-based firepower are expected to proceed at a pace commensurate with technical advances in airpower—perhaps reducing the dependency of ground forces on air support, depending on the coalition elements' technical base. The ability for ground forces to overwhelmingly engage an opponent will always be a goal of the ground commander, and commanders will always plan engagements to optimize usage of their available power. Unforeseen opportunity is frequently a product of warfare. Maintaining the flexibility of tactical forces ensures exploitation of good fortune and rapid response to good fortune's evil twin—bad luck. Regardless of doctrinal issues about the best way to employ airpower, there will always be opportunity to influence the ground battle directly from the air with air-to-ground weapons. The most likely first priority of airpower in future conflicts will be to attain air and space superiority, either concurrently with or immediately following the shock delivered by the initial strategic attack. Attaining air superiority allows a fluid reapportionment of air and space assets. Single-mission tactical aircraft are luxuries not likely to be affordable, given today's evolving fiscal realities. The ability of available air-to-air assets to swing to ground attack will maximize the application of power.

In the year 2025, the inevitable evolution of precision weapons will make every air asset that is capable of ground attack capable of performing CAS. The automated assignment of the ground target coupled with ease of employment and standoff capability will profoundly simplify weapon delivery tactics and defensive system requirements. The addition of onboard and in-flight programming capabilities greatly enhances mission effectiveness. Relative proximity of the target to allied ground troops poised for attack could be the only discriminator of mission demarcation between CAS, battlefield air interdiction, or even strategic attack. Premission planning and weaponeering time will be slashed. The resultant rapid apportionment flexibility will revolutionize the application of airpower.

## Chapter 1

# Introduction

Opportunities to make quantum leaps in warfare are rare, but they are upon us today. Due to demonstrated and anticipated advances in technology, the ability to project a survivable weapons delivery platform into heavily defended airspace over a target is rapidly diminishing. The use of standardized standoff weapon systems significantly improves delivery platform survivability. Current and forecast growth in the capabilities of standoff weapons are inadequate to maximize their potential. From the outset, the weapons must be considered as only a part of an airpower system. This white paper discusses the many elements of such a system. It is critical that this entire system be defined as early as possible to allow for concurrent procurement programs for its constituent parts.

In the interest of bounding the problem, only air deliveries of air-to-ground mechanisms near friendly forces are considered here. As the name implies, close air support is the use of airpower in proximity to friendly ground troops to complement their scheme of maneuver. It is apparent that many of the technologies discussed in this paper have surface-to-surface applications. Military objectives and available assets drive the need for target engagement by air firepower in addition to ground-based firepower. The technological evolution in outlying years does not diminish the need for the unique aspects of airpower and space power in the battlefield—and the deep strikes—of the future.

Close air support functions as a series of tasks and systems to accomplish the mission. Figure 1-1 shows the sequence of the four attack tasks. These elements are common to many different missions as they are defined today. It is obvious in the development of the recommendations contained in this paper that these systems capabilities may render some mission paradigms obsolescent. The resultant method for applying airpower produces a

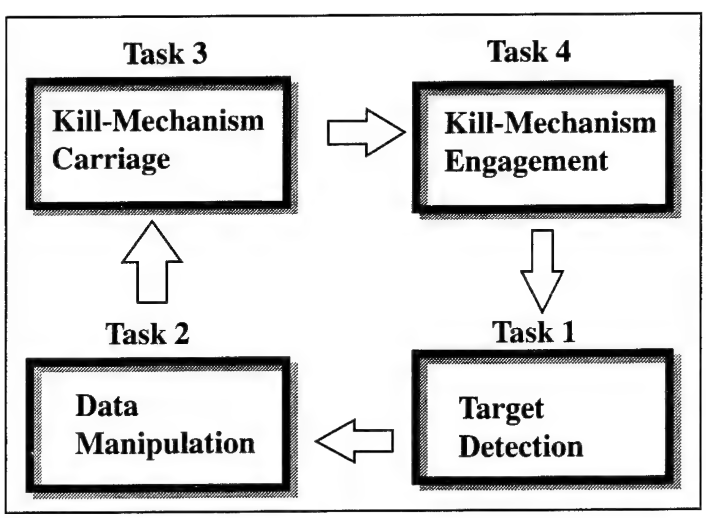



**Figure 1-1. Close Air Support Task Loop**

seamless transition across those paradigms. For academic completeness, there is a discussion of CAS and its current definitions and methods. It is important to note that CAS is just one of the many ground-attack missions. It is useful to review the following discussions of current capabilities and limitations in this context.

Targeting, command, control, communications, computer, and information ($C^4I$) data, kill mechanism carriage, and engagement are the four tasks associated with CAS. Targeting refers to detection, identification, and tracking. $C^4I$ permits prioritizing and directing our air assets while disseminating needed information to all levels of command. Currently, manned aircraft comprise our kill mechanism carriage. In the future, air assets other than manned platforms will comprise the majority of delivery vehicles used in CAS. Kill mechanism engagement refers to weapon assignment, desired effects, initialization, release, acquisition, onboard processing, tracking, and fusing of the payload.

# Chapter 2

# Current and Required Capabilities

All services define CAS similarly. Appendix A presents the independent service definition and its source. They all stress that CAS is air action against hostile targets in close proximity to friendly forces. To varying degrees they stress that it needs to be timely and flexible, and that it requires detailed integration with the fire, movement, and location of friendly ground forces. The proximity of friendly forces to targets makes fratricide a real concern. CAS accomplishment requires close integration with ground forces to aid their scheme of maneuver. It is important to realize that CAS is *not* independent air action against the enemy where there are no friendly forces. Missions flown in Bosnia during 1995, for example, should not be classified as CAS.

## Close Air Support Description

Today's close air support mission requires a one-on-one relationship between the delivery platform aircraft and the ground tactical representative to employ weapons in close proximity to friendly forces. To produce this relationship in a timely and efficient manner requires a complex command and control network. Appendix B has a more in-depth discussion of the current means for conducting CAS. CAS planners and operators must have a thorough understanding of joint and service operating procedures. In addition, they must understand service communication requirements, delivery platform capabilities, and weapon effects. Significant limitations to CAS effectiveness (e.g., target identification, the threat of fratricide, and the operating environment) prevent full exploitation of the capabilities offered by airpower on the battlefield. Appendix C describes these limitations more fully.

## Close Air Support Issues

The CAS debate will be entering its 80th year in 2025. The Army and the Air Force disagree over several issues about how to conduct CAS. Mission allocation priorities, target tactics, timeliness, night and weather capabilities—all constrain CAS effectiveness. Proposed service-specific solutions are the source of this rift. The Army feels that Air Force allocation and acquisition priorities neglect CAS in favor of air superiority, interdiction, and strategic strike.[1] However, the realities of 2025's battlefield will force an accommodation between the two sides. The Army will acknowledge that CAS aircraft cannot loiter inside the enemy's antiaircraft envelope and expect to survive. The lethality of 2025 antiaircraft weapons will place greater demands on aircraft operating around enemy troops. After action reports on Desert Storm showed that CAS aircraft (A-10s and AV-8Bs) suffered the highest number of combat losses.[2] Uninhabited aerial vehicles (UAV) can currently loiter over a battlefield to provide reconnaissance data to collection agencies. These vehicles are readily adaptable for ground-attack missions, especially when a significant antiaircraft threat exists. This fulfills the Army's need for ubiquitous airpower presence.

Army doctrine demands high-tempo, 24-hour-a-day, all-weather operations. Current CAS shortfalls in poor weather and night conditions capability make Army planners reluctant to plan operations where Air Force firepower integration is essential to mission success. Consequently, the Army has often excluded CAS from their scheme of maneuver. These environmental limitations to CAS will be overcome by 2025, making CAS more dependable.

Currently the Army is concerned that "immediate response" CAS is not responsive enough to the Army field commander and his scheme of maneuver.[3] The Army desires on-call, near instantaneous assets, even if that means holding back those assets from accomplishing multiple missions. The Air Force wants to take full advantage of the high sortie rate of combat aircraft and not hold back assets on the chance they might be needed.

Several improvements by 2025 will serve to mitigate CAS shortfalls. Weapons will be more versatile; the same weapon will be able to reconfigure to fragment for soft targets or penetrate for hard targets. Consequently, mission tasking will be less restricted by aircraft weapons load. Weapons will have greater ranges and standoff capability. All surface-attacking aircraft will be capable of precision weapons delivery in weather or at night and will therefore be CAS-capable. Ground commanders and aircrews will have access to the information from a common network that will electronically model the battlefield. The next chapter describes that network.

**Notes**

1. Raoul Archambault and Thomas M. Dean, "Ending the Close Air Support Controversy" (Newport, R.I.: US Naval War College, 21 June 1991), 8–11.

2. John T. Correl, ed., "More Data from Desert Storm," *Air Force Magazine* 79, no. 1 (January 1996): 62–66.

3. Archambault and Dean, 14.

## Chapter 3

# System Description

In 2025, a ground force element nominates targets via the battlenet without regard to how they will be attacked. The ground force elements are concerned with effect and criticality. The battlenet is a system of systems that collects data from multiple sources, fuses the data, turns data into information, and continuously updates battlespace situational awareness for all users. Furthermore, it provides a comprehensive communications network for the commanders involved in combat to synergistically direct the fight as well as a means for the war fighters to execute and report.

As the battle unfolds, enemy units confronting the ground commander cause direct conflict with the planned scheme of maneuver. Other units not yet on the scene may also threaten the plan. The commander will have a display (a miniature 3D model) of the battlespace (provided by the battlenet). The commander may customize the battlenet display to present only relevant information and forces. Via this battlenet, the ground commander designates targets for destruction, containment, or immobilization, and the timing of such effects. Artificial intelligence (AI) imbedded in the battlenet, as programmed by cognizant authority, will inventory available friendly forces and task weapons systems to engage the enemy within microseconds. The battlenet component on board a manned platform receives the tasking, acknowledges the assignment, adds the targets to a customized display of the battlespace, and recommends a course of action to the operator. If no friendly system is available at the required time, the battlenet presents various options to the ground commander. It may suggest changing the timing of the attack, the desired effect, retasking another assigned unit, or relaying a request for additional force to the next higher commander on the battlenet. Higher levels of command may hold forces in reserve to answer these requests. Human oversight is available at all levels to provide a robust backup system and to ensure that artificial intelligence and scheme of maneuver remain in concert. The battlenet will be used by all levels of command and operations, from the commander in chief (CINC) monitoring the theater campaign down to the engaged tank commander. The tank commander uses the battlenet to request additional targets or for assistance in disposing with the present batch.

The nominator of the target may not be physically in the area of operations. In fact, the tasking order may direct CAS not by sortie but by weapon and vulnerability time over a region. This, combined with all-weather weapons, will make CAS constantly available to the battlespace commander. An aircraft on an interdiction mission may be tasked by the battlenet to deliver some of its weapons in a CAS scenario, requiring the platform to ingress over a certain area at a specified time to expend the selected weapons en route to the interdiction target. Weapons or sorties could be shifted to other missions by the battlenet when it determined that the weapons were no longer needed for CAS. In fact, any aircraft transiting near a ground unit could be tasked by the battlenet for any or all of its weapons to aid in an engagement. The battlenet provides a means for shifting aircraft to higher priority targets at any time. This would be normal, and would be a part of routine training. Human operators coupled with battlenet logic decide whether the new target has high enough priority to warrant diverting or delaying a platform.

## Background and Assumptions

In the world of 2025, the Air Force operates at considerable distance from the United States over periods ranging from weeks to months.[1] High-tempo operations will be conducted around the clock, unaffected by weather conditions. With the formation of new nations and changes in the world order, the United States will not know when or where the next conflict may appear, who will be fighting, or whether they are recognized government forces, nongovernmental organizations, or insurgent groups.[2] Technological advances in all fields will provide a vast array of improvements in materials, computing power, sensors, and weapons. One downside to these technological improvements is that they will be available to almost everyone interested in obtaining them. It is reasonable to assume that today's emphasis on reduced costs, reduced collateral damage, and short-duration involvement will continue in the future. A CAS system in the future (fig. 3-1) must be able to cover large distances and be able to loiter well away from the target area, yet be able to penetrate a highly defended threat zone consisting of surface-to-air missiles, directed energy weapons, stealthy aircraft, and attack from space.[3] In addition, the system must be able to support operations in environments from thick jungle to urban areas against all types of adversaries, ranging from heavily armored, fast-moving shock forces to crowds in the heart of a major city. Two issues central to CAS—proximity to friendly forces and rapid delivery of weapons—will not change. Forces will still need to "close" with each other to achieve a tactical decision. Closing with each other is obviously a relative term, since weapons of the future may have tactical ranges well beyond those of today. The effectiveness of future weapons requires rapid response from our systems to prevent high casualty rates.

## Target Detection

A major limitation of CAS today is the requirement for the forward deployed spotters to visually sight enemy vehicles or troops before bringing in air support. "Because smaller units will be capable of massing decisive effects on future battlefields, there will be a greater need in the 21st century for our forces to become less detectable to the enemy" and, conversely, to make the enemy far less opaque to us.[4] Human observers on the battlefield become less and less effective as

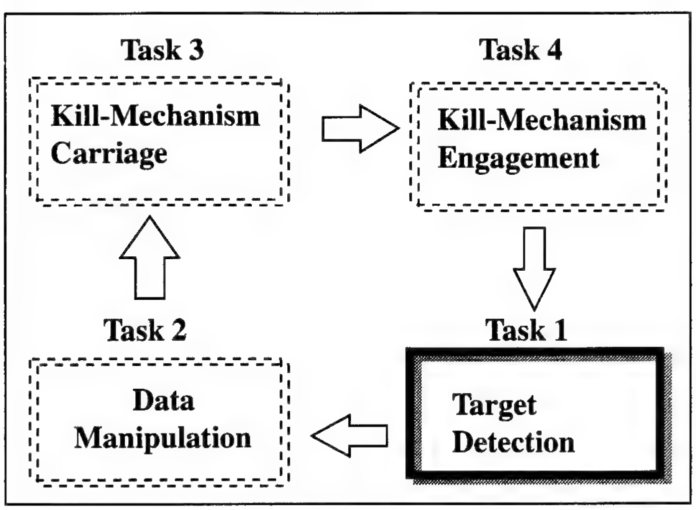



**Figure 3-1. Target Detection Tasking in CAS Loop**

forces become smaller, more maneuverable, and lethal. Current intelligence outputs give the ground commander the general location of an enemy force, but not in near-real-time and not with great accuracy, especially if the targets are in motion. Battlespace commanders in the future must have near-real-time enemy dispositions, movements, and intent if at all possible. Our commanders must have continuous knowledge of the presence of individual vehicles prior to their arrival in the battlespace commanders' area of influence until they are in close contact with friendly forces. Uninterrupted coverage of target vehicles and personnel in all types of weather, on any terrain, or in an urban environment, should be the minimum level of performance in 2025. Force XXI's concept of operations dovetails with this philosophy and states that our required capabilities hinge on leveraging information-linked technologies, particularly sensor fusion, robotics, fuzzy logic guidance, and control.[5] Following a preliminary operational analysis on CAS as a system, the following criteria were identified as the most important in target detection and tracking:

1. target location accuracy; less than 10 meters preferred
2. environmental availability; detection 24 hours a day in all weather and terrain
3. target location update; situation dependent zero to six hours.[6]

In order to satisfy these and other requirements, the United States must develop new sensor technology. One candidate system utilizes space platforms as the primary means of surveillance. However, a system based entirely on satellites poses some formidable problems. Orbital distances create signal attenuation, loiter time, area coverage, and power supply problems for satellites. Elements of the radar equation exact great concessions from a space-based system in terms of power requirements, signal-to-noise, and resolution.[7] Very large structures will be required to generate the power required by these systems, a fact which negates the desired design feasibility, cost savings, hardness, and maneuverability desired from orbital platforms. "The next generation of American spy satellites should be able to provide virtually continuous 24-hour coverage of a battlefield anywhere in the world. Even further into the future, they may be able to distinguish friend from foe by 'licking' the battlefield with a laser so that commanders can follow the movements of their own forces as well [as] those of the enemy."[8] This type of system could be expensive, and commanders would likely use these satellites for higher priority missions.

Upgrading existing airborne platforms such as joint surveillance target attack radar system (JSTARS) and the airborne warning and control system (AWACS) will provide some improved capabilities over the next 10 to 15 years. However, relatively small area coverage, operational inefficiencies, high operating costs, vulnerability, and limited number of these aircraft will hamper their operations and reduce their usefulness. The uninhabited reconnaissance aerial vehicle (URAV) proposed in *New World Vistas* appears to be a cost-effective solution when employed either as an independent system or in conjunction with other airborne and spaceborne platforms. URAVs can be outfitted with a wide variety of multispectral sensing equipment—such as synthetic aperture radar (SAR), light detection and ranging (LIDAR), optical viewers, or laser radar—and then deployed to loiter at very high altitudes for extended periods without refueling. Already a current electro-optical system suitable for installation on a fighter-sized platform produces "tactically significant imagery" up to 60 miles away from the target.[9] URAVs working in conjunction with manned platforms and satellites could easily provide continuous and detailed coverage of the area of interest.

URAVs can work cooperatively with satellite constellations by projecting high-power radio frequency (RF) beams over the area of interest. The satellites receive

reflected signals from targets near [on] the earth to form a distributed bistatic SAR system (fig. 3-2). Clutter rejection is improved because of the varying reflection angles to different satellites. Moving and fixed targets can be detected with high resolution as the result of the long baseline between satellites. This arrangement limits the number of expensive spaceborne transmitters by reducing coverage to a specific area of interest.[10]

This mixture of satellites and URAVs produces resolutions under 10 meters and continuous coverage over a given area of interest. Drawbacks to this system are the complexity and susceptibility of URAVs to attack or malfunction, the requirement to have multiple aircraft on call, and the possibility of leaving an area unmonitored.

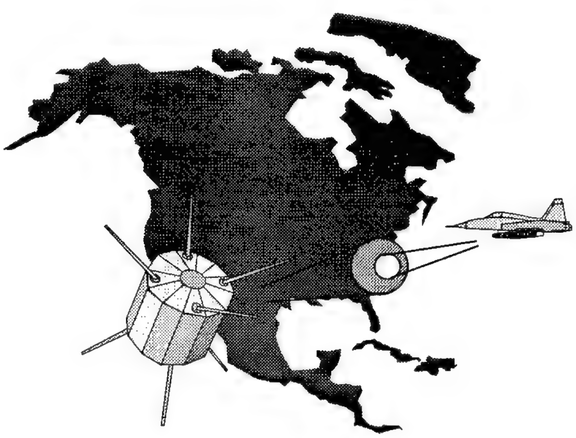


**Figure 3-2. BiStatic Target Detection**

Remote sensing in synchronization with or in the absence of airborne or space platforms utilizes surface arrays of small camouflaged disposable sensors capable of transmitting data to collection platforms.[11] Sensors can exploit the full electromagnetic spectrum, detect forms of mechanical energy such as seismic or acoustic signals, and physically analyze diverse sets of chemical and biological components.[12] Artillery, missiles, or airborne platforms dispense the remote sensors, automatically recording their locations. Signature data transmitted by the sensors to the battlenet become identified targets with speeds and vectors. Active detection devices such as directed-energy transmitters may alert the targets of the presence of sensors, therefore the commander must have the option of passive sensing if targeting effectiveness is adequate.

We must develop a network of ground-based sensors, high-altitude unmanned platforms, and surveillance satellites as recommended by the *New World Vistas* study.[13] The battlenet must then provide this intelligence to all levels of command with continuous updates including near-real-time battle damage assessments.

## Concept of Operations

Locating and tracking a fast-moving vehicle made of light-weight nonmetallic materials powered by a quiet, cool engine may be very difficult. This problem is made even more difficult if the vehicle has radar/infrared (IR) low-observable technology and onboard countermeasures capable of deceiving radar or laser tracking systems. According to the Army, vehicles on the future battlefields will have these characteristics.[14]

Satellites with multispectral sensor suites will locate enemy forces well before their probable contact with friendly units. A battlenet collects data from multiple sources, such as signals, imagery, emissions intelligence, and remote sensor inputs, then fuses the data and continuously updates the battlespace picture. Cycle time between updates depends on the orbit or the number of satellites in the net. Air-breathing UAVs supplement intelligence collection by providing updates to enemy movement over a wide area or focusing on a particularly difficult tracking problem. The battlenet that is providing information to the commander decides when to increase the frequency of observations and adjusts orbital flyovers or activates air-breathing platforms as required to maintain accurate target locations. When commanders, at any level, need more detailed information, they direct the battlenet to provide it and the

battlenet chooses the method. A robust system depends on multispectral sensing from each sensing platform in order to accommodate different target types and ambient conditions. As friendly and enemy forces close on each other, cycle time for system updates shrinks to zero, requiring a continuous flow of data into the battlenet. Potentially large target densities found in armored battles or urban crowd control operations dictate that the battlenet be able to discriminate individual vehicles or personnel from among larger target sets. UAVs supplement battlespace coverage at this point, and the battlenet controls their actions. The sensor suite on manned vehicles automatically selects the proper sensor or combination of sensors to compensate for target type, terrain, light, and weather, and then displays the image via a pilot's helmet-mounted cueing system while passing the information to the battlenet. In an autonomous mode the system could find targets, identify them, and then launch weapons without human intervention.

A detection system must be capable of thwarting countermeasures created by target systems. Visual spoofing, such as holographic displays, would fail to pass a multispectral imaging process as they would not create thermal, magnetic, electromagnetic, or acoustic returns.[15] False thermal sources also fail to pass through multispectral gates and discriminators. Artificial intelligence (AI) queries the system to find if target motion or activity matches known behavior and checks for countermeasure activity. Adaptive learning by the battlenet compensates for new countermeasures fielded by an enemy by adapting the sensor suite without human intervention.

### Target Identification (Combat Identification)

Future weapons systems must possess the capability to operate cooperatively with non-US forces in standoff engagements using smart weapons while preventing collateral damage from friendly fire.[16] The United States will continue to be a major exporter of weapons to other countries; therefore it is reasonable to expect future enemies to come equipped with equipment similar to our own. Automatic target recognition (ATR) technology must progress to the point where accuracy, reliability, and unambiguous target recognition allow application of lethal force with nearly 100 percent assurance of target identification.[17]

The primary characteristics required of a combat identification (CID) system are accuracy, reliability, and security. The desired system must exhibit close to 100 percent accuracy, reliability under all operating conditions, and security in order to prevent the enemy from mimicking or denying us the identification capability. As a corollary to accuracy, the CID system must be robust enough to utilize any identification systems of civilian police forces, coalition members, or allied nations. Allied forces may present problems to our systems since equipment may not be standardized or even fielded by the respective nations. Coalitions, by their ad hoc nature, present several complications (e.g., language barriers, dissimilar equipment, and limited time) to us in distributing our system for use during rapidly developing scenarios.

For this discussion, CID systems fall into two main categories: active-cooperative and passive. An active-cooperative system requires a transponder affixed to the vehicle or person to transmit a response to an interrogation; much like the battlefield combat identification system (BCIS) currently undergoing testing by the Army. The BCIS actively queries and responds to similarly equipped vehicles in all weather conditions with up to 99 percent accuracy.[18] In the future, responses to interrogation should be multispectral; utilizing acoustics, IR, visual bands, RF, millimeter wave, and laser beams. Active systems have several problems associated with them. One is reliability. Unless the system is 100 percent reliable, possibilities exist for fratricide in combat. Antennas and other external

devices (the BCIS uses an externally mounted transponder) may be blown off during combat, rendering the system useless. Another problem is security. If an enemy can read, jam, or duplicate the incoming or outgoing signals, the system's effectiveness becomes severely degraded. If the signals are not of a low probability of intercept (LPI) nature an enemy is likely to be able to localize emission sources and target them. It is also reasonable to expect that some of our systems will fall into enemy hands, therefore our system must be reprogrammable. A different type of active system does not require interrogations but periodically transmits required information such as identity and status in the blind. This information "strobing" would have to be spectrally unique to prevent detection, but could simplify the overall system and allow one half of the ID equation to remain passive.

Semipassive systems do not utilize transponders or transmitters to reply to interrogations. Instead an interrogator reads the identity from a tag or label of some type on the vehicle or person. For example:

> Spacecast 2020 suggested using techniques that it likens to "licking" and "tasting" to identify objects on the ground. The licking would be done by a laser beam fired from a satellite which would be equipped with sensors that would "taste" the spectrum of the radiation reflected back from the target. By comparing this with a database of know tastes it would be possible to identify an object. Friendly tanks and aircraft could be coated with a chemical that produces a characteristic spectrum when excited by energy of a certain frequency or other characteristic.[19]

A totally passive system requires the use of naturally occurring emanations such as acoustic, thermal, or RF energy from a target. Another type of system scans for characteristic signals reflected from offboard illumination of the target (visual light, distortion of magnetic fields, or bistatic imaging systems). Computerized pattern recognition is a current and evolving technology.

In all likelihood, in order to achieve near 100 percent accuracy, the CID system of 2025 needs the capability to both actively and passively discriminate enemy from friendly and combatant from non-combatant.

**Concept of Operations.** In 2025, friendly troops enter the battlespace with their personal identifiers.[20] The identification mechanisms could be in the form of microchips worn by or imbedded in the soldiers and chemical implants injected into the body or grown externally.[21] Microchips must be capable of transmitting a response to interrogations in an active mode. In a passive mode, the presence of a chip containing the correct code detected by a sensor acknowledges identification. Chemical or Defense Nuclear Agency (DNA) sniffers detect the desired chemical in a soldier or the existence of a particular organic material grown on the soldier's body. The same principle could be applied to vehicles. A molecular patch of material imbedded in the vehicle provides a passive method of ascertaining its identity. A variety of multispectral transponders provide active recognition to battlenet queries. Enemy troops and vehicles may be identified by default. If the battlenet knows the locations of every friendly troop or vehicle and can identify noncombatants, then anything else detected is declared hostile unless designated by the battlespace commander.

Sensors locating objects in the battlespace have the ability to identify the object if directed by the battlenet. One type of system utilizes pattern recognition logic to pick out pieces of data coming from sensors and comparing the data to previously stored signatures to identify enemy troop formations and even individual vehicles. If information needed by the system is not available, the system directs other platforms or sensor types to reconnoiter the area in question.[22] An active or passive system could identify friendlies by reading a label attached to an object via numerous methods. As the battlenet sensors

detect each target in the battlespace, they apply a physical label to the target. For example, a particle beam imprints coded information on the exterior of specially painted vehicles or irradiates the clothing of exposed personnel. Labels placed on targets could be magnetic, optical, or electronic, and can be sized down to the molecular level. The label contains data that includes the type of target, date time group, and military unit controlling the vehicle or person.

The system must be robust enough to utilize the identification systems of allied forces during coalition operations. Sensors would be required to interrogate an unknown transponder, analyze the response, and determine if the response came from a friendly system or a designated hostile system. If the interrogator receives a response that does not correspond to known friendly systems or fails to receive a response at all, the interrogator activates a separate series of identification methods involving discriminators such as material composition, acoustic, electromagnetic, or vibration signatures. For situations involving a mixture of hostile forces and noncombatants in an environment where no external evidence distinguishes the two (a riot or urban disturbance for example), the system may need only distinguish between friendly "tagged" personnel and others. Current electro-optical sensors can discriminate individuals for positive identification at ranges up to three miles; by 2025, it is reasonable to postulate ranges an order of magnitude farther away.[23] Pattern recognition logic could assist in threat determination, based on discriminators such as vehicle type, color, and motion, or note whether personnel are carrying weapons, moving in a tactical manner, and so forth.

The battlenet fuses information from a wide variety of sources to bring the confidence factor of the target identity to near 100 percent. The battlenet transmits its confidence factor with the target identity to commanders, thus providing them with crucial engagement data.

### Target Tracking

Target tracking is handled as a category, separate from detection. A complete CAS system must be capable of not only finding and identifying objects in the battle space but keeping track of them as well. Tracking systems capable of flexible update cycles maintain contact with designated targets throughout extensive maneuvering during close contact with friendly forces. As with detection, robust tracking systems utilize a mixture of space-based platforms, UAVs, and ground sensors to accomplish the mission.

**Concept of Operations.** Space-based platforms, URAVs, or remote sensors identify an enemy force in the battlespace commander's area of interest. Sensors identify the number and type of targets as well as the status of the force. A designator mechanism physically brands each target by placing a magnetic, laser, or other detectable code on the object. Various identification mechanisms read this tag and update the battlenet with target location. If a handoff from the original detection platform to subsequent sensors occurs, the follow-on sensors read the target codes and feed current locations and vectors into the battlenet, thus updating the system. Targets not showing up during repeated update cycles cause the battlenet to provide additional scrutiny from search sensors as the system attempts to relocate the objects. Remote ground sensors providing target information to the battlenet may be equipped to read the identification codes already placed on each target, place a designator, or merely pass existent data to the battlenet. Weapon guidance mechanisms would have the capability to acquire and track these specific identity codes. Tactical platforms capable of continuous real-time target tracking interface with the battlenet to maintain the picture; thus, the battlespace commander or anyone requiring immediate target locations may access the

information.[24] Multiple platforms managed by the battlenet follow selective target tracking, lists to preclude or provide selective redundant tracking, thereby giving the battlenet a capability to resolve conflicts caused by multiple ground observers locating and designating the same target.

Depending on the level of information required, the battlenet provides each user a display of all or a portion of the battlespace to include friendly and enemy locations as well as terrain features, target types, and target status (destroyed, pending destruction, untargeted). Display methods vary from helmet-mounted displays to laptop-sized units in the hands of soldiers to large, room-sized units where commanders can move or see anywhere on a "virtual" battlefield.[25] For manned aircraft, the pilots' virtual visor presents the picture outside his cockpit in any direction. The picture includes target location, aircraft parameters, threat locations, weapons status, and friendly locations.

The battlespace commander authorizes the battlenet to service a target in whatever manner desired. Since the battlenet maintains continuously updated target files, the system chooses a method, weapon, and platform. It then launches and, if necessary, guides the weapon to the target. Battle damage and resulting target effectiveness are displayed as soon as the battlenet processes the data.

## Command, Control, Communications, Computers, and Information

The success of future CAS hinges on effective command and control (task 2 of fig. 3-1). This integrated system must appear seamless to ground units and to the joint aviation targeting process. According to out year projections of doctrinal concepts (*Sea Dragon* and *Force XXI)*, United States Marine Corps (USMC), and United States of America (USA) operational doctrine will diminish the importance of linear forward line of troops and fire support coordination line concepts by 2025. Both services envision a greatly expanded amorphous and opportunistic battlefield, with small units operating in great breadth and depth supported by indirect fire. It is a battlefield with no front, rear, or flank, where detection results in engagement. Multiple sources, ranging from forward-deployed ground forces to battlespace commanders thousands of miles from the battlefield, input indirect fire requests to the battlenet. Target input will be to battlenet by data burst or similar low-signature transmission. Commanders, with significant assistance from the battlenet, conduct target analysis for appropriateness, deconfliction, validity, and availability of aviation assets. When the battlenet receives instructions to engage a target, the battlenet assigns a delivery platform and transmits necessary information directly into the fire control system. Weapon and navigation programming are automatically accomplished while the platform proceeds to release points. If the situation dictates, the ground commander may direct the weapons platform to contact a ground or airborne controller for "danger close" or degraded deliveries. Partial failures in the battlenet allow graceful degradation to 1995 doctrinal-style CAS. The battlenet also allows multiple levels of interoperability with coalition partners.

## Battlenet System

Human input to the battlenet comes from a variety of equipment (fig. 3-3). All sources, whether they are laptop computers or handheld radios, are secure and jam-resistant. Operators gain access to the battlenet after providing identification that the battlenet recognizes. Key cards and code words are simple forms of identification that are easily distributed to operators. Fingerprint recognition or voice matching are more complicated methods of identification that can be used to gain access to the battlenet. Voice-to-data converters provide unprecedented freedom to the operator by allowing

direct voice contact with battlenet computers. Built-in redundancy against single-point cataclysmic failure permits graceful systemwide degradation and partially shields operators from the effects of enemy attacks. Filtering data, and automatic situation-updating of the dynamic 2025 battlefield present two major challenges to a battlenet system. Various command levels will have different available information and display presentations are possible. System designers must analyze the vulnerability and requirements. Virtual reality, holographic, and multifunction personal display device efficiency of centralized versus decentralized processing systems.

A horizontal command and coordination network integrating aviation and ground operations ensures quick response to CAS-type missions. The elimination of intermediate decision levels lessens delays caused by administration and processing procedures. The transparent injection of CAS missions into other sorties further enhances CAS timeliness.

**Concept of Operations**

Input from the sensor network builds a situation map in both digital and visual formats. The battlenet updates friendly, neutral, and enemy locations to the level of detail required to keep pace with their movement through the battlespace. Various levels of command have access to varying degrees of information, dependent on need and security requirements. The battlespace commander engages enemy units as required to accomplish task force missions. As enemy units move (or in a worst case "pop up") closer to friendly ground units, a variety of sources place CAS requests into the battlenet. The battlenet displays the information to the battlespace commander and a decision to engage follows. All levels of command, from the battlespace commander down to the ground tactical leader, receive a regularly updated target status from initial detection and engagement to postmission battle damage assessment (BDA). Mission specifics such as location, description, time-on-target (TOT), routing, and target layout are sent to the delivery platform. Computers produce an

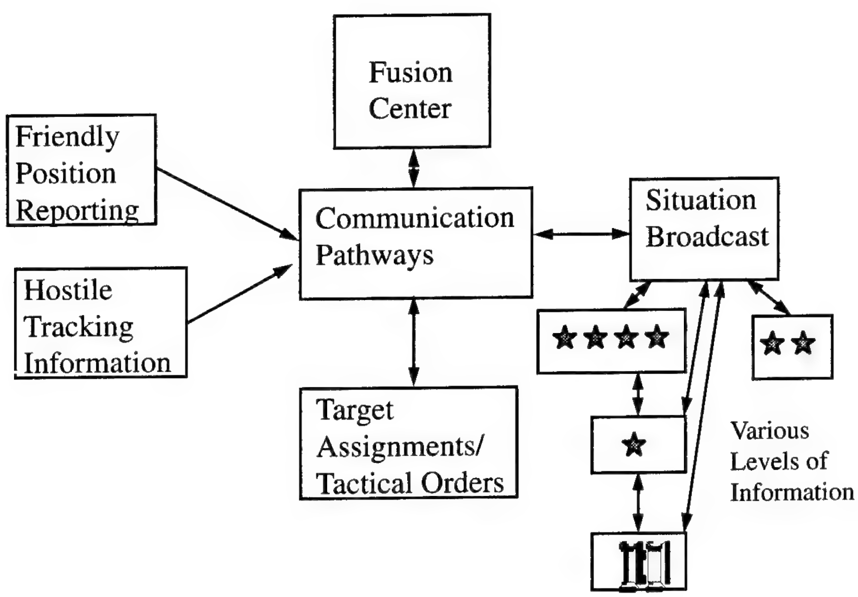



**Figure 3-3. C$^4$I Network**

optimal route to the target, taking into account terrain, threats, and a host of other factors. The battlespace commander possesses the ability to amend the mission until weapons impact. The command hierarchy establishes an authorization priority to preclude conflicting commands. This allows for late changes or mission aborts in case of unforeseen deconfliction problems. A capability to introduce last-minute changes to CAS missions, or even weapon trajectories, reduces the potential for air-to-ground fratricide incidents. After weapon impact, the battlenet conducts multisensor BDA to determine mission success and reattack requirements.

## Kill-Mechanism Carriage

The "battleplane" of Douhet, a stealthy high-altitude, high-speed bomber that can shoot down incoming missiles, reflect high-energy weapons, rain destruction upon the enemy, and remain affordable probably will not exist. Thirty years is generally insufficient time to procure another new-technology bomber. Current trends in aircraft acquisition time and cost, combined with increased congressional oversight, legal battles, and smaller budgets, virtually guarantee that most of the airframes flying today will still be flying in 2025. Note that the A-6, B-52, C-130, and C-141 flew during Vietnam and are still flying today. Thirty years will elapse from the time the F-15 became operational until its replacement, the F-22, is operational—assuming no further delays. President Jimmy Carter canceled the B-1 program in favor of a stealth bomber almost 20 years ago. However, a fleet of fully operational B-2 stealth bombers, the block 30s, has not been completely fielded. Lost investment and legal battles over the cancellation of the A-12 program and the Supercollider serve as examples for more oversight. Bureaucratic requirements and approvals result in less risk-taking, which ultimately further slows a lethargic acquisition process. Shrinking defense budgets offer fewer incentives for contractors to champion new products. The consequence to the war fighter is older airframes with more upgrades and improvements. The year 2025 may yet see an F-16 block 80, F-15F, or a B-2 block 40 aircraft. Forecasts show the venerable B-52 to remain in service until 2040.[26] Budgetary constraints may find the United States purchasing only manned aircraft that are currently past the demonstration and validation phase (e.g., the F-22, V-22, and possibly the Joint Strike Fighter). New-technology demonstrator aircraft will also be in existence in the test environment, but not in operational units.

Demands on aircraft systems remaining in the 2025 inventory include greater aircrew situational awareness, augmented countermeasures, better threat identification, greater standoff range, and improved weapons performance. Improvements in miniaturization and processing power will open new opportunities for communications, information processing, weapons, and UAVs. Future uninhabited combat aerial vehicles (UCAV), viewed as cheaper alternatives to manned aircraft, are expected to significantly exceed today's capabilities. However, UCAV procurement faces some of the same acquisition challenges that manned aircraft face. Hopefully, the promise of an order of magnitude leap in performance over current manned aircraft with the prospect of affordable costs will spur the development of UCAVs.[27]

By the year 2025, astrotrackers, terrain matching systems, and improved inertial navigation systems (INSs) will offer relief from the growing dependence on the global positioning system (GPS) yet preserve the navigation accuracy demanded by sophisticated weapon systems. Aircraft navigation computers will store detailed maps of the planet's surface, the location of minute gravity anomalies, and an electronic order of battle. A highly accurate navigation system and a detailed map of the planet provide the means for aircraft to fly nap of the earth passively. Future advances in artificial intelligence and cockpit enhancements permit a significant workload

reduction, thus enabling aircrews to devote more time to avoiding the threat and attacking the targets. Greater tactical flexibility will be achieved through better three-dimensional displays of the local combat environment, enemy weapons engagement zones, weapon ranges, and the disposition of forces.

Improved communications and computer capability with a preponderance of smart stand-off weapons give all surface attack aircraft, as well as aircraft not necessarily considered tactical, the capability to conduct CAS. Notable improvements in weapon performance create a mission for essentially an airborne truck. The truck, a UCAV, helicopter, F-22, or B-52, simply hauls weapons to a launch point and initiates a mass attack or an individual weapon launch on demand.

Tactical delivery platforms equipped to carry iron bombs and a gun still have a place in 2025, possibly for no other reason than the fact that these weapons are so numerous, reliable, and cheap. At the high end of the technology spectrum, directed-energy weapons installed on 2025 gunships (progeny of the AC-130U) offer the possibility of surgical destruction on a variety of targets. As replacement costs for aircraft grow prohibitive, more will be spent on survivability, resulting in an expanding spiral. Ultimately, even strategic bombers need the advantage of being able to shoot back when a venerable but upgraded MiG-21 serendipitously stumbles into a successful intercept.

Many of the same measures used today to evaluate CAS aircraft carry over into 2025. Parameters reflecting superior performance may not be the ones we recognize today. However, aircraft range, speed, weapons capacity, and delivery precision are easily measurable. These characteristics initially answer the question, "Can the aircraft do the job?" Weapon system lethality, aircraft survivability, vulnerability, hardness, and stealthiness form the core characteristics used to address compatibility between aircraft and mission. These measurements, although more important than simple performance factors, are much more difficult to assess quantitatively. Cost, maintainability, and reliability will still be important discriminators, and they will remain under the watchful eyes of the military, Congress, and the media. In the future, aircraft value will be highly leveraged against its capacity to accommodate multiple roles. Single-mission aircraft become a luxury too expensive to be affordable. Flying qualities, critical in the past to aircraft selection, will be less important during initial assessment and selection. Software-driven flight control systems, such as in the F-16, C-17, and B-2, permit operators to rapidly modify aircraft flight characteristics.

Information is the high ground of the twenty-first century.[28] Consequently, new critical measures of merit for aircraft will be pilot vehicle interface, human factors, controls, displays, and data fusion. Successful CAS requires fusing data, processing data into information, and timely display of useful information to the aircrew. The absence of quality, easy-to-use controls and displays increases aircrew workload to the point that CAS becomes impossible; the aircraft truly becomes all Mach and no vector. Placing a premium on operational flexibility and lowering aircrew workload during cockpit upgrades results in maximum aircrew effectiveness. Designing from scratch and using automation as an end instead of means are formulas for disappointment—or at the least, very expensive programs. Aircraft test programs, such as the B-2, have rediscovered that failure to transfer the lessons learned from other aircraft such as the F-16C, F-18, F-15E, or F-117, and building automated systems around a rigid, single-focused mission, creates an architecture that is labor-intensive and has little operational flexibility.[29] Flexibility is the foundation of CAS and airpower. An aircraft with no flexibility has no utility in accomplishing the CAS mission. By 2025, fiscal and operational realities will drive the require-

ment that all strike aircraft, including heavy bombers, be capable of supporting CAS.

## Kill-Mechanism Engagement

This section addresses how munitions apply to the 2025 CAS mission (task 4 of fig. 3-1). First, it describes CAS munition characteristics, current weapons, and development trends. Second, it describes future weapon developments and enabling technology required for the CAS mission. Finally, this section addresses possible munition countermeasures and counter-countermeasures.

Weapon performance in 2025 will require the same core capabilities as in 1996. Currently, CAS weapons must affect enemy battlefield targets in ways defined as both desirable and advantageous to friendly ground troops. Traditionally, the military limits this association to target destruction. Friendly forces do not always require, or even desire, the complete destruction of an enemy target. This holds true for the entire continuum of targets, from individual soldiers to massed tank formations.

The Vietcong, for example, found it sometimes beneficial to severely wound or maim US troops rather than kill them outright. Wounding a soldier had the added benefit of degrading his unit's effectiveness by saddling his fellow soldiers with his protection and care until his evacuation. In another example, we can destroy the mission effectiveness of a radar-guided, surface-to-air missile (SAM) through electronic jamming of acquisition or tracking elements, as opposed to physical destruction with a bomb. Additionally, jamming may be more cost-effective and less risky than attempting a hard kill. We therefore, conclude that target characteristics and ground force needs will drive the requirements of CAS weapons in 2025. As previously stated, this does not always equate to target destruction.

Keeping the above discussion in mind, we now address some CAS weapon characteristics that will be required in the next 30 years. First, weapons must produce the desired effect on the target. This characteristic can span the entire range, from vaporizing targets to merely rendering them ineffective for certain periods. Second, CAS weapons of 2025 must have the flexibility to engage several individual types of targets during one mission. Budget constraints no longer allow for the fielding of specific weapons for each type of battlefield target. As a result, we need to develop weapons that have the flexibility to adapt to changing mission requirements. These changing requirements include an ability to engage a vast array of target types as well as the ability to produce a varied spectrum of effects on those targets. A third characteristic of future CAS munitions will be interoperability between large numbers of delivery vehicle types and different military services or nations. Compact and lightweight construction translates to increased delivery platform performance as measured in range, number of weapons carried, loiter time, maneuverability, and survivability. A final CAS weapon requirement is an ability to lower threat exposure to the carriage platform during the delivery sequence. CAS becomes truly viable only if we can ensure an acceptable risk-to-gain ratio during its execution. Designing standoff munitions that do not expose delivery vehicles to high-threat environments is one way to increase survivability.

The US military is developing two systems to provide a CAS capability in the future: the joint direct attack munition (JDAM) and the joint standoff weapon (JSOW). JDAM is a low-cost, GPS-aided, inertial guidance kit that is attachable to unguided Mk 83 (1,000-lb), Mk 84 (2,000-lb), BLU-109, and I-2000 deep penetrating bombs.[30] This jointly developed munition attempts to increase the accuracy of weapons types currently in inventory without increasing disproportionately their overall cost. JDAM uses a guided-bomb tail kit to provide GPS updates to a dumb Mk-80-series bomb to increase the bomb's accuracy during the

delivery phase of its use. Estimated JDAM accuracy falls in the 10-to-12-meter range, making it an "accurate weapon" but not a precision weapon.[31] Weapons such as laser-guided bombs are considered to be precision munitions because they produce a very small if not zero circular error probability (CEP). JDAM will be much more cost-effective than true precision munitions against targets that do not demand a zero CEP. JDAM demonstrates an improvement in desired target effects and interservice interoperability over current Mk-80-series munitions. This is the beginning of the trend toward the future weapon characteristics discussed earlier.

JSOW consists of various submunitions carried on a nonpowered, aerodynamically efficient airframe. This frame is constructed of composite and aluminum materials with nonfolding fixed and moveable tail surfaces and folding wings. Submunitions carried include the BLU-97A/B combined-effects submunition, the BLU-108 sensor fused array submunitions, and a preplanned product improvement unitary warhead.[32] The weapon's design served to further meet the necessary characteristics of future CAS munitions by addressing the flexibility, desired effect, interoperability, and threat exposure issues.

2025 CAS must be conducted in a cost-effective and survivable manner. Planners and operators must exercise caution before exposing a multimillion-dollar aircraft to a high-threat level for any sort of mission. This threat exposure is necessary in today's environment because the delivery platform/munition combination is not capable of delivering weapons in a manner that shields the delivery platform to a sufficient degree.

There are three approaches to addressing this problem. The first is to develop weapons delivery platforms that are inherently less vulnerable to the fielded threat. An example of this is the current emphasis on stealth technology and self-protection systems. The second is to develop munitions deliverable from outside the lethality ring of the fielded threats. Examples of this are weapons such as the Tomahawk cruise missile and other standoff munitions. The third approach is a combination of the two.

The three approaches described above cover a wide spectrum of cost, with the first option representing a very high price tag for the delivery vehicle and the second representing a high cost per weapon. There are inherent advantages and disadvantages to both extremes. As the price of the munition or delivery platform increases, the number obtainable with a fixed budget decreases. Senior leaders must wrestle with classic quantity-versus-quality decisions. It is important to remember, however, that the combination of weapons delivery platforms and munitions must be of a quality that is sufficient to have a high probability of accomplishing the mission but also of a quantity that is sufficient to be able to take out the volume of anticipated targets. Too few high quality weapons systems are as disadvantageous as an unlimited supply of ineffective low-quality systems. The purpose here is to identify weapon characteristics in 2025 that strike the necessary balance between the quality and quantity extremes.

Keeping the above in mind aids in identifying several key aspects of 2025 munitions. Weapons for 2025 permit the assignment of target and desired effect data to the weapon while onboard the platform or after release. As a result, weapons allow onboard or in-flight reconfiguration of their effect mechanism. To make the weapon truly effective requires flexible guidance options and delivery methods. Developing a fairly high degree of quality and capability into each weapon while maintaining a very high level of ability to engage a wide array of targets and employment scenarios is extremely important.

Although a high level of capability tends to increase the cost of each weapon, the high degree of flexibility achieved allows the same results with a much lower overall inventory of munitions. This allows

additional savings in areas such as logistics, storage, transportation, training, and maintenance. As a result, these savings can defray increases in the cost of weapons due to their increased sophistication and capability, thereby allowing more weapons to be procured. The end result is an overall decrease in the quantity and types of weapons but an increase in their overall capability and utility. This translates to increased survivability of the delivery platform, thereby reducing the number of delivery platforms required in the force. In essence, a smaller but more capable force structure. The classic example of this reasoning is seen in the combat capability of hundreds of B-17s during World War II (WW II) compared to the effects of just one F-117 carrying two bombs in the Persian Gulf War. These two weapon systems produced similar effects on their targets.

Achieving the anticipated gains in weapon capability requires advancements in computer, guidance, and explosive technology. Weapons used in the 2025 CAS environment must overcome two current limitations of today's weapons. First, they must be dispensed from a platform likely to be well away from the battlespace and not in direct view of the target. Since the delivery vehicle may be anywhere in relation to the friendly and enemy positions, future munitions must be accurate enough and reliable enough to dispense with bomb fall line and aircraft run-in restrictions. Second, they must be able to identify, track, and achieve desired effects on a variety of target types autonomously. Guidance packages and seeker systems permit targeting the weapon or changing targets while onboard the delivery platform, after release, or late in the terminal guidance phase. Battlenet targeting information includes specific target characteristics such as exposed armor aligned linearly north to south in a 50 x 300-meter array and a specific weapon assigned to the target. Each munition provides its own identity to the delivery platform, hence to the battlenet, so that each munition may be independently targeted.

Active or passive seekers will be onboard-selectable. An active seeker illuminates the target by a multispectral source such as radar, laser, or optics. Active illumination of the target by the weapon requires guidance to the target from onboard navigation systems or steering from the battlenet until the weapon reaches acquisition range and begins terminal phase guidance. This guidance could include an on-munition target CID interrogator, or a system able to read the labels installed on enemy vehicles outlined in the previous section. Longer range and endurance CAS weapons require a target recognition system capable of identifying target signatures and characteristics. Passive guidance requires the battlenet to guide the weapon through all phases of flight into contact with the target. Since the battlenet already identified and tracked the target, the system could issue precision guidance instructions to the weapon. Passive guidance includes the ability of the weapon to read and identify multispectral signatures, either independently or in conjunction with the battlenet, then home in on the source of the signatures. Weapon susceptibility to countermeasures is on par with the battlenet. If necessary, the weapon cross-checks target location with the battlenet to resolve inaccuracies. Weapon guidance system degradation should be graceful and nonlethal. A malfunctioning guidance package requests and receives assistance from the battlenet, a manned platform, or a ground controller. If a malfunction prevents the weapon from accurately recognizing or tracking a target, the weapon deactivates and/or initiates low-order, self-destruction before impact.

The munitions of the future will be lightweight and multipurpose. Inflight conversion from a unitary warhead to submunitions or mines allows inherent targeting flexibility. In addition, battlenet input and onboard target recognition features allow flexible yields from the unitary warhead. Dual use of

the stored energy material as an explosive or propellant would allow tactical trades of energy expenditure against the target or increased standoff ranges. Submunitions exhibit independent target acquisition capabilities. A nonexplosive kill mechanism such as hypervelocity darts reduce the complexity of the weapons package, but they still require a guidance package to get them into position to accelerate into the target. The capability must exist to target individual enemy troops in close proximity to friendly forces and incapacitate or kill them without exposing friendly troops to the weapons effects. Steerable flechettes or directed-energy weapons fired from overhead uninhabited platforms could have this effect.

CAS in urban environments or during peacekeeping missions requires the option of using nonlethal weapons. Acoustic signals, microwaves, sticky foam, or mood-altering pheromones could be dispensed. The caveat here is that friendly troops must have the inherent ability to resist the effects of these weapons because they may not know the type of weapon being used, hence may not have time to prepare. Special ear plugs, nose filters, or uniforms become standard equipment for this type of engagement. *New World Vistas* envisions an autonomous miniature munition (AMM) which is a small (100 pounds), highly effective unitary munition providing a force-multiplying capability over a wide range of air-to-surface tasks.[33] Perhaps the AMM offers suitable nonlethal effects packages for use in these special environments. However, getting the AMM to be truly effective requires rapid progression in ATR, adaptive lethality, onboard guidance, and maneuvering packages.[34]

### Concept of Operations

Modularity in the buildup of flexible munitions (FM) results in a customized weapon tailored to a specific target, or similar subset of targets. A truly effective FM uses a hybrid material that provides a range of released energy effects on a target and doubles as a propulsive source for stand-off applications. Modularity can also reduce cost by allowing a specific sensor, guidance, and stand-off mechanism to be used as tasked by the battlenet. This reduces multi-capability redundancies that frequently drive up costs.

A self-contained FM production system (fig. 3-4) could be used to rapidly respond to battlenet requests for customized weapons.

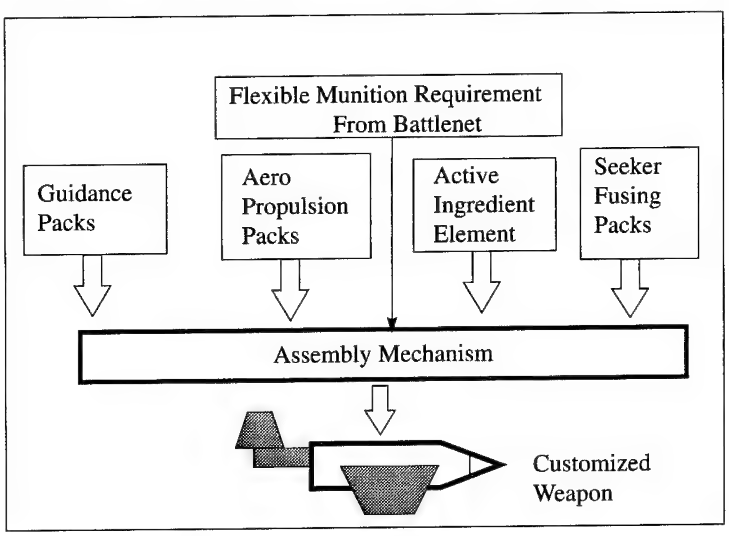



**Figure 3-4. Flexible Munition Production Pallet and Subsystem**

By producing the weapons "just-in-time," storage and manual assembly of weapons could by eliminated.

Location of the system could vary from internal carriage in larger aircraft when their use is warranted, to flight-line or forward-operating-base use for smaller aircraft (fig. 3-5). In large aircraft, the greatest flexibility would be realized since little to no weapons carriage structure would be required. The weapon would simply be produced and expelled in a continuous process. In smaller aircraft, a universal carriage mechanism is desired. In either case, support for the system would be replenishment of high-use subcomponents.

In summary, the battlespace of 2025 may be very different from that of today. However, the four subtasks of air-to-ground attack will remain. The goal of any system will be timely and precise firepower. Reduction of effort and simplification of combat tasks for the human components during high stress will reduce the "fog of war" and allow the human to better deal with the results of "friction."

**Notes**

1. USAF Scientific Advisory Board, *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 5.
2. Ibid.
3. Ibid.
4. "Force XXI America's Army in the 21st Century," *Army Focus*, September 1994, 13.
5. Ibid., 40.
6. ***2025*** Operations Analysis Team interview, Air University, 14 March 1996.
7. *New World Vistas*, summary volume, 23.
8. Vincent Kiernan, "The Eyes That Never Sleep," *New Scientist* 148, no. 2002 (4 November 1995): 510.
9. David A. Fulghum, "Long Range Sensor Offers Options," *Aviation Week & Space Technology* 139, no. 2 (12 July 1993): 23.
10. *New World Vistas*, summary volume, 22.
11. ***2025*** Concept, no. 901093, "Continuous Area Surveillance and Denial," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).
12. "New World Vistas," sensor volume (unpublished draft), i.
13. "New World Vistas," attack volume (unpublished draft), x.
14. Ibid., 40.
15. ***2025*** Concept, no. 901175, "Holographic Image Projector," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).
16. "New World Vistas," munitions volume (unpublished draft), 66.

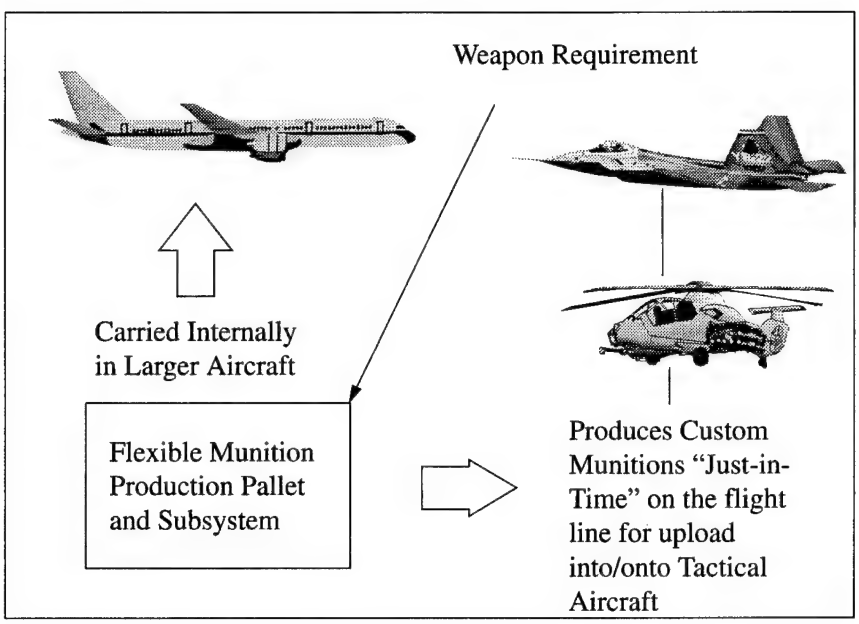



**Figure 3-5. FM Multiple Uses**

17. "New World Vistas," sensor volume (unpublished draft), ix.

18. "New Electronic Device Developed to Prevent Friendly Fire Incidents," *Defense Electronics* 27, no. 3 (3 March 1995): 12.

19. Kiernan, 13.

20. Scott R. Gourley, "U.S. Army Warriors: 21st Century Equipment for 21st Century Missions," *Defense Electronics* 27, no. 1 (January 1995): 14.

21. ***2025***, Concept, no. 901165, "Personal Tactical Organizer," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

22. ***2025***, Concept, no. 901151, "Model Based Situation Database," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

23. Micheal A. Dornheim, "New Sensors Show Two Paths to Reconnaissance," *Aviation Week & Space Technology* 143, no. 2 (10 July 1995): 48.

24. ***2025*** Concept, no. 901131, "Real Time Battlefield Video," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

25. ***2025*** Concept, no. 900913, " Virtual Battlefield Assessment Integrator," ***2025*** Concepts Database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

26. Richard Aboulafia, "A Bomber Force Unrivaled," *Aviation Week & Space Technology* 144, no. 2 (8 January 1996): 17.

27. David A. Fulghum, "ARPA Explores Unmanned Combat Aircraft Designs," *Aviation Week & Space Technology* 144, no. 9 (26 February 1996): 23–25.

28. "America's Army—Into the 21st Century," *Army Focus 1994*, September 1994, 1–8.

29. James C. Dunn and Donald L. Wiess, "B-2A Flight Test Progress Report," *Society of Experimental Test Pilots Symposium Proceedings* 1995, 17–33.

30. David A. Fulghum, "Pentagon Cuts Field of JDAM Candidates," *Aviation Week & Space Technology* 140, no. 15 (18 April 1994): 22.

31. Ibid.

32. Mark G. Chauret, ed., "Air Combat Command Operational Concept for the Joint Standoff Weapon (JSOW)," 28 March 1994, draft, 4–5.

33. "New World Vistas," munitions volume (unpublished draft), 10.

34. Ibid., 11.

## Chapter 4

# Concept of Operations

The underlying basis for this entire concept is the battlenet. It must exist either in physical form or as an assembly of computational elements in cyberspace. Access to and modification of individually desired architectures must occur at the first indication of need. Ideally, configuration and access requirements would be preplanned and "on the shelf" at the joint planning cells. Any service makes airpower assets (aircraft, weapons and personnel) available to the CINC. The need for tactical mission planning is small and the need for weaponeering is negligible. Aircraft loaded with FMs await a signal from the battlenet to launch. Platforms receive instructions (via datalink commands) to either fly to a point (to await CAS-type assignment) and hold, or to fly to a point and relegate commit authority to the battlenet. Weapons release occurs to engage targets enroute or upon reaching a turnaround point. The battlenet assigns a weapon to a target, then passes FM configuration data to the individual weapon via the carriage platform. The platform releases individual weapons or groups of weapons during various portions of the flight. The same aircraft may drop one or two weapons while crossing an area with troops in contact, drop all but a few against strategic targets, and drop its remainder against an emerging target during its return to reload.

### Employment

To initiate a CAS mission, the requester first contacts the battlenet and provides proper authentication. After providing target data and desired effect to the battlenet, controllers receive a target correlation confirmation, proposed time on target (TOT), and a request for release authorization. The controller, perhaps someone many leagues from the target, confirms this information, authorizes weapon release, and awaits target engagement. The controller would either personally evaluate target condition after the attack or receive that information from the battlenet, which could use multiple sources of data to better determine residual effectiveness of the target. Figure 4-1 depicts this process. For interdiction or strategic attack, the same process could occur with the controller being replaced by anyone, anywhere, with access to the battlenet as authorized by the JFACC.

### Communications, Logistics, and Personnel Requirements

Current communications methods use multiple bands of the RF spectrum. This makes directional detection of transmissions fairly easy. Using LPI techniques helps minimize the possibility of detection. Using other spectral regimes offers security and redundancy. Burst transmissions use the time domain for similar benefits.

Use of tracking software allows business and industry to monitor the transshipment status of materials. Satellite tracking of shipment and inventory control transponders will provide similar capability on a global scale. Logistics tracking subsystems of the battlenet provide additional information to battle managers, with AI-monitored flags available to warn of impending shortages.

Personnel management tasks in 2025 take on even more significance due to lower overall manning levels. Training must be continuous as new applications of technology take hold. As reliance on technology increases, the ability to gracefully degrade to less automated modes becomes very important. Commanders must ensure that personnel do not lose the capability to revert to manual operations if the system becomes

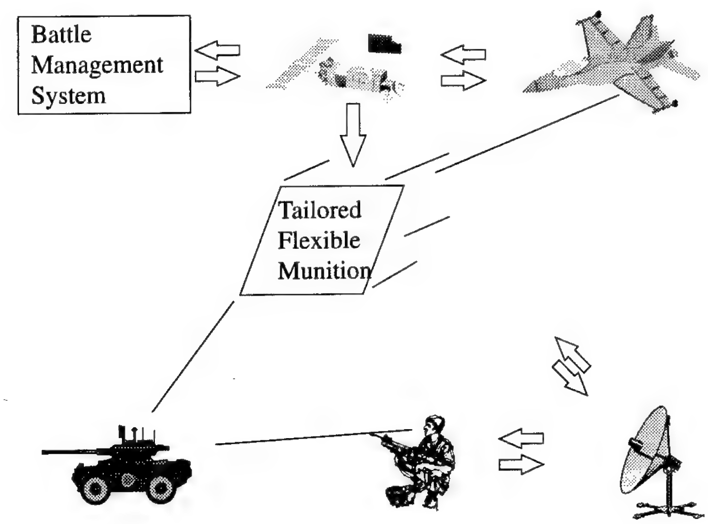



**Figure 4-1. Battlenet**

degraded. If the battlenet breaks, do the troops know how to call in air support?

Strategically, reduction of the human risk element in many combat environments may increase the willingness of political leadership to employ combat power. The effects of the dehumanization and mechanization of warfare will carry profound philosophical implications. The "push-button" warriors forecast in the seventies became the "video" warriors forecast in the early nineties. By 2025, technically motivated remote control advocates may cause a shift in perception regarding the use of deadly force. The images and realities regarding the inhuman nature of any form of warfare may be the first elements of information filtered from the battlenet. Impersonal employment of death-producing effects, from safe and cozy command centers by those not willing to accept personal risk, fundamentally changes the face of conflict. The moral implications are immense.

## Countermeasures

As targeting, $C^4I$, weapons, and delivery systems evolve, the US military must expect improvements in enemy countermeasures to these systems. Some of the countermeasure methods, such as destruction, deception, jamming, and intrusion, overlap into several of the functional task areas. Negating the effects of the countermeasures may require different methods, depending on the functional area affected.

Central to the concept of CAS in 2025 is a battlenet for data input, information management, targeting, and command and control. A decentralized battlenet keeps critical nodes to a minimum, but that will not prevent a sophisticated enemy from targeting the net. Severing the input sources from the processing units involves blocking data transmissions, cutting communications uplinks, or electronically separating the data source from the data processor and information from the receiver. Therefore, the system must be resilient enough to withstand these efforts. The battlenet must accept a variety of input methods; for example, a controller with a voice radio should be able to call in target information to the battlenet. The system accepts and converts the spoken words into digitized information used by the battlenet.

If an enemy developed the ability to produce false targets, he could pose several

different levels of threat. First, the volume of target information may overwhelm the battlenet itself. Second, the target indications could cause human battlespace commanders to commit weapons to invalid targets. Electronically placing real targets in the wrong location is a technology that is readily available now. If an enemy creates false targets and the battlenet recognizes them as being false, then his forces would be immune from attack if he physically or electronically disguises vehicles and personnel to resemble the false targets. We will not be alone in the technology race. A likely scenario provides a peer competitor access to the same weapons and technology we have. Security of information-based systems must remain a top priority.

Long-range enemy UAVs patrol deep in our territory looking for ours. Air-to-air and surface-to-air weapons systems will inevitably become more sophisticated in their ability to detect, track, and shoot down aerial and even space platforms. This indicates either a need for us to develop small numbers of well-defended platforms with resultant complexity or, perhaps, larger numbers of simple and redundant platforms networked so that losses do not critically affect operations. An effective method of preventing CID poses serious threats to our ability to conduct CAS operations. Compromise of critical capabilities and subsequent reproduction of CID signals could be devastating. Future CID systems should avoid using single-mode interrogation techniques.

The capability for graceful degradation must be built into any system to permit the battlespace commander to authorize weapons release based on targets input by sources outside the battlenet; for example, the forward controllers on the ground. If a threat successfully falsifies its position or prevents detection by our sensors, then command and control could reduce to the forward controller with a pair of binoculars and a radio calling in air strikes.

Perhaps the worst thing the enemy can do to our system is to cause errors in the determination of his location. In 2025, weapons will be small and sophisticated. They travel to targets using offboard systems, onboard guidance, or a combination of the two for midcourse and terminal guidance. A reduction in the size of weapons in 2025, plus the possible high cost of placing terminal sensors on each munition, creates an argument for placing command guidance packages on some weapons. These weapons remain under the control of the battlenet and receive offboard guidance all the way to impact. Therefore, if the battlenet has incorrect information on the target location by even a few meters, the likelihood of successful target engagement decreases.

Enemy vehicles of the future—and even personnel—may carry a close-in-self-defense system incorporating a target detector, tracker, and kill mechanism. Once our weapon succeeded in finding its way to the target, it would still run the risk of being intercepted and negated in the last few hundred meters. Our weapons must be too quick, too agile, too smart, or a combination of all three. By smart, the weapon must be able to sense and react to outputs from the target such as lasers, radar, particle beams, or projectiles. Reaction consists of maneuvering by the weapon, closing its eyes for a short time, deflecting or disrupting the enemy's defensive weapons, or targeting the source of the enemy's defensive system.

In any event, the continuous cycle of countermeasure and countercountermeasure is prohibitively expensive. In fiscally limited environments, the risk exists that threat reactions to system development and deployment are ignored. The easiest method of preventing countermeasure development is to highly classify the newly developed capability. But this carries an increased price tag in security costs, and is in fact a tenuous solution. Compromise of any capability, especially in an information intense era is almost inevitable.

The best method for ensuring war-fighting superiority is to have an acquisition strategy that includes preplanned program

improvements and that tests the system in a realistic operational environment. Testing acquired threat systems against ours demonstrates system strengths and weaknesses. The increased use of modeling and simulation runs the risk of missing a hidden threat capability or, just as bad, overestimating a threat capability and wasting precious resources to counter a nonissue.

## Joint, Coalition, or Noncombatant Operations

Systems proposed in this paper must be available to all US forces. Service-unique requirements must not result in reduced joint usage. Various forms of US systems should be made available to our coalition allies. Transparent sophistication will allow for rapid incorporation into any country's forces.

Nonlethal forms of air-delivered weaponry will have direct application in civil disturbances or operations-other-than-war (OOTW). The ability for the battle manager to rapidly apply various levels of precise power to a complicated target arena will provide for a much larger range of risk-management options.

# Chapter 5

# Investigative Recommendations

To improve close air support in 2025, the Department of Defense should focus its research and investigation on the three main areas listed in table 1: battlenet, weapons, and aircraft.

The information revolution comes to CAS in the form of the battlenet, a network of sensors, computers, communications, and displays. The most important element for development within the battlenet is a reliable combat identification system. The lack of CID and the fear of fratricide make CAS extremely difficult, and training intensive, and they generate employment tactics not conducive to aircraft survival.

Modeling the battle and manipulating information will require new controls and displays. Hardware for displays being developed in the civilian sector will probably be sufficient for military needs. However, the mission-essential software may not be. There are some fundamental differences between the military and civilian computer-operating environments. Speed and clarity are important in both environments. Five minutes to achieve a completely accurate solution may be quite reasonable to a civilian but intolerable in combat, where an 80 percent solution is acceptable if given in five milliseconds. Most civil applications allow for the operator to focus undivided attention on the data presentation. The combatant operating in a rugged environment under great stress faces life-threatening distracters. He or she will not have time to call up a file manager while sitting comfortably at a desk out of the line of fire. Combat cannot tolerate time spent searching through different pages or levels of software for enough information to formulate an overall picture. There is no such thing as a combat file manager.

Data cannot be dumped on warriors; it must be converted to information, then

**Table 1**

**Recommended Research Areas**

| AREA FOR RESEARCH | COMPONENT |
|---|---|
| Battlenet | Combat Identification |
| | Controls and Displays |
| | Sensors |
| | Datalinks |
| | Artificial Intelligence |
| Weapons | Standoff Range |
| | Terminal Guidance |
| | Nonlethal |
| | Flexible Configuration |
| Aircraft | Uninhabited Aerospace Vehicles |
| | Situational Awareness |
| | Performance/Survivability |

pushed to the combatants, thus allowing them flexibility in determining quantity and format. Customized displays on a variety of mediums are absolutely essential to the war fighters. Programs must pursue the lessons learned from related works and projects when designing controls and displays. Keep one eye focused on maintaining flexibility. This is especially true in a world where electronic obsolescence can occur in a few months while new weapons are introduced every few years and aircraft are expected to last decades.

The B-2 program managers elected not to transfer the lessons learned from previous aircraft developments in developing a new software architecture. A rigid, constrained, focus on a single mission unnecessarily increased aircrew workload to the point that it was rated marginally acceptable before the demanding or complex evaluations could be flown.[1] Experienced organizations designing from scratch, following old paradigms, or new inexperienced organizations may be prone to offer what works in an office, machine, process, or game as a solution to the military's needs. Meeting military demands requires robust testing, demonstrated flexibility, and expandability for all types of systems. Continuing progress in the development of artificial intelligence and computer processing power by the civil sector should provide the requisite technology to comply with the military's unique needs to convert data to easily accessible information.

Our senior leadership's vision of the future must motivate substantial investment in reconnaissance and surveillance sensors and platforms. In the future, the multitude of sensors and platforms must be melded into an overarching architecture that supports the battlenet concept. As the battlenet generates improved situational awareness for all echelons of command, the demand for additional information increases. Therefore, the system of sensors providing data to the battlenet must permit room for rapid growth and expansion.

The string, composed of communications and datalinks, ties the pieces of the battlenet together. Security, speed, and bandwidth require ongoing research and development.

Integrating improved weapon systems into the battlenet will vastly increase the capability of US forces to accomplish CAS. By 2025, all combat aircraft gain the ability to accomplish this mission 24 hours a day, regardless of the weather. Increased standoff range, quantum improvements in terminal guidance, sensing, and fusing enhance weapon effectiveness. Targeting flexibility and nonlethal capabilities add new dimensions to CAS operations. In the future, the air tasking order (ATO) may task individual weapons vice actual aircraft.

The current evolution of aircraft is proceeding on the right track. The Department of Defense (DOD) is correctly placing emphasis on developing uninhabited and remotely piloted vehicles. These are the weapons platforms of the future. We will be able to find, identify, and attack targets at lower risk and ultimately lower cost via these platforms. Manned aircraft, however, will not be eliminated by 2025. Accordingly, we should continue to pursue improvements in aircraft performance and stealthiness. These improvements, however, are not the only means of enhancing combat effectiveness. The construction of the battlenet, weapons advancements, and better automation will greatly improve and prolong aircraft combat effectiveness. Improvements that enhance situational awareness will provide the maximum return in combat capability.

The acquisition process is the foundation for much of this improvement. We need an improved cost-effective process that fields technology quickly and supports oversight requirements. The civilian sector aids this process by accomplishing most of the initial research and development. Unfortunately, new developments also aid our enemies, hence we must be able to exploit civil technologies before our adversaries do.

Current acquisition methods are acknowledged to be unwieldy and unnecessarily restrictive. In the emerging era of extremely rapid technology growth, the acquisition system must accelerate to maximize the benefits of new capabilities. The phenomenon of "obsolescence while in development" is a very real hazard. The process also requires continued reform in the face of shrinking defense dollars and the defense industrial base. Using concurrent developmental and operational test processes reduces time and funding requirements. Detailed modeling and simulation techniques can accurately predict system performance. Operational suitability of future systems will be much easier to test due to the inherent reliability of electronic systems.

A strategic development plan and common architecture must be agreed upon at the earliest planning stages to provide a framework on which to construct independent elements. Concurrent development of subcomponents must occur to shorten the acquisition cycle.

Service parochiality and fights for scarce fiscal resources must be avoided at all levels. Joint procurement processes must continue to be required at every possible opportunity. However, as we arrive at the battle in 2025, we know there are austere funding environments enroute. Maintenance of the US military's supremacy in the future will require constant improvement in both technologies and practices. A constant maximum effort must be made by every member of the profession of arms to continually optimize the vast capability of this force, regardless of uniform color, and blind as to which service operates which system. To do less shirks our sworn duty.

## Note

1. Col James C. Dunn and Donald L. Wiess, "B-2A Flight Test Progress Report," *Society of Experimental Test Pilots Symposium Proceedings*, 1995, 17–33.

# Appendix A

## Close Air Support Definitions

Close Air Support enjoys a similar definition in each branch of the service. These definitions came from several sources and were cross-referenced. This appendix presents the definitions in the following format:

**Branch Of Service**

Source of information

Reference where source discovered information

Text of information

**USAF**

Air Force Manual 1-1, *Basic Aerospace Doctrine of the USAF*, vol. 2, March 1992.

Joint Pub 1-02

> Air action against hostile targets which are in close proximity to friendly forces and which require detailed integration of each air mission with the fire and movement of those forces.

US Army FM 100-20, July 1943

> Air participation in the combined effort of the air and ground forces, in the battle, to gain objectives in the immediate front of these ground forces.

Joint Force Air Component Commander (JFACC) Primer, 2d ed., February 1994.

Joint Pub 1-02

> Close support—action against targets or objectives sufficiently near the supported force as to require detailed integration or coordination of the supporting unit.
>
> Close Air Support: Supported Commander: JFLCC
>
> CAS Targeting: JFLCC
>
> Coord Air: JFACC
>
> Graphically CAS is depicted as air-to-surface operations between the forward line of troops (FLOT) and the fire support coordination line (FSCL)

The United States Air Force, *A Dictionary*, ed. Watson and Watson (New York and London: Garland Publishing, Inc., 1992).

Department of Defense, Department of the Air Force, *The United States Air Force Dictionary*, ed. Woodford Agee Heflin (Montgomery Ala.: Air University Press, 1956).

David Poyer, *The Med.* (New York: St. Martin's Press, 1988).

> Close Air Support (CAS) is action against enemy targets that are close to friendly forces. It requires the detailed integration of each air mission with the fire and movement of the enemy forces. Close air support is requested and approved by the support unit commander, and is controlled by the forward air controller.

Department of Defense, Department of the Air Force, Air Force Pamphlet 50-34, *Training: Promotion Fitness Examination Study Guide*, vol. 1 (Washington, D.C.: Headquarters US Air Force, 1990).

Department of Defense, Department of the Air Force, *The United States Air Force Dictionary*, ed. Woodford Agee Heflin (Montgomery, Ala.: Air University Press, 1956).

> Close Air Support Missions support land operations by attacking hostile targets close to friendly surface forces. Close air support can support offensive, counteroffensive, and defensive surface force operations with preplanned or immediate attacks. All preplanned and immediate close air support missions require access to the battlefield, timely intelligence information, and accurate weapons delivery. Close air support enhances land force operations by providing the capability to deliver a wide range of weapons and massed firepower at decisive points. It can surprise the enemy, create opportunities for the maneuver or advance of friendly forces through shock action and concentrated attacks, protect the flanks of friendly forces, blunt enemy offensives, and protect the rear of land forces during retrograde operations.

**JOINT/MARINES**

Joint Pub 3-0, *Doctrine for Joint Operations*, 1 February 1995.

Joint Pub 1-02

> Air action by fixed and rotary wing aircraft against hostile targets which are in close proximity to friendly forces and which require detailed integration of each air mission with the fire and movement of those forces. Also called CAS.

**ARMY**

United States Army, *A Dictionary*, ed. Peter Tsouras (New York & London: Garland Publishing, Inc., 1991).

Department of Defense, US Army, FM 44-3, *Air Defense Artillery Deployment: Chaparral/Vulcan/Stinger* (Washington, D.C.: Headquarters, Department of the Army).

FM 17-50, *Attack Helicopter Operations*, 1984.

FM 101-5-1, *Operational Terms and Symbols*, 1985.

FM 100-27, *USA/USAF Doctrine for Joint Airborne and Tactical Airlift Operations*, 1985.

> **Close Air Support** is air action against enemy targets that are located close to friendly forces. Thus, the detailed integration of each air mission with the fire and movement of the enemy forces is required. Close air support is requested and approved by the support unit commander, and is controlled by the forward air controller.

Department of Defense, US Army, FM 100-5, *Operations* (Washington, D.C.: Headquarters, Department of the Army, 1986).

FM 100-27, *USA/USAF Doctrine for Joint Airborne and Tactical Airlift Operations*, 1985.

> **Close Air Support Missions** support land operations by attacking hostile targets in close proximity to friendly surface forces. Close air support can support offensive, counteroffensive, and defensive surface force operations with preplanned or immediate attacks. All preplanned and immediate close air support missions require access to the battlefield, timely intelligence, information, and accurate weapons delivery.
>
> Close air support enhances land force operations by providing the capability to deliver a wide range of weapons and massed firepower at decisive points. It can surprise the enemy, create opportunities for the maneuver or advance of friendly forces through shock action and concentrated attacks, protect the flanks of friendly forces, blunt enemy offensives, and protect the rear of land forces during retrograde operations.

FM 100-26, chapter 3, "Air Support Operations"

> **Close air support** is air attacks against hostile targets that are in proximity to friendly ground forces and that require detailed integration of each air mission with the fire and movement of those forces. The fixed wing CAS strikes are controlled by an element of the tactical air control system (TACS) operating with the supported maneuver unit. This element is responsive to the needs of the commander of the ground unit.

**NAVY**

The United States Navy, *A Dictionary*, ed. Bruce W. Watson (New York and London: Garland Publishing, Inc., 1991).

Department of Defense, Joint Chiefs of Staff, Joint Pub 1-02, *Department of Defense Dictionary of Military and Related Terms* (Washington, D.C.: 1985).

DOD, US Naval Education and Training Command, NAVEDTRA 10368-F2, *Air Traffic Controller 1&C* (Washington, D.C.: 1983).

NAVEDTRA 10367-G, *Air Traffic Controller 3&2*, ed. James T. Pruett (Washington, D.C.: 1983).

NAVEDTRA 10479-C2, *Seabee Combat Handbook*, ed. Patrick J. Essinger (Washington, D.C.: 1985).

**Close Air Support** is air action against hostile targets that are close to friendly forces and that require detailed integration of each air mission with the fire and movement of those forces.

# Appendix B

## Close Air Support Description

All the services use the same joint definition of CAS. CAS gives the ground force commander the ability to engage the enemy with the combined arms of ground and air forces to gain synergistic effects over the battlefield and its targets. To accomplish this integration, the ground commander gains access to the air component's planning and execution process. Specialized communication nets tie these leaders into the normal ATO process and also provide the ability to get crisis response on short notice requests.

All US armed forces doctrinally conduct CAS very similarly, although the CAS joint publication is currently being written. CAS is centrally controlled and decentrally executed. The higher unit commander approves missions and then the forward air controller (FAC) and delivery aircraft actually controls final execution. This allows the air component commander (ACC) to allocate his air resources in compliance with the joint force commander's (JFC) direction. To accomplish this, an extensive command and control ($C^2$) network has to be used. CAS differs from air interdiction by its proximity to friendly ground forces and the need for detailed integration of each mission with the fire and maneuver of those forces. Due to concern over fratricide, constraints have been put in place to protect ground forces (mark and clearance to drop). These constraints limit tactical flexibility of the delivery aircraft.

Currently, CAS can be divided into the following $C^2$ nodes:

| System | Current Agency |
|---|---|
| 1. Terminal Controller | FAC (ground or airborne) |
| 2. Ground $C^2$ System | Fire Support Coordination Center (FSCC) |
| 3. Aviation $C^2$ System | Tactical Air Command Center/<br>Tactical Air Control Center(TACC)/<br>Direct Air Support Center (DASC) |
| 4. Delivery Platform/Weapon | Aircraft |

The terminal controller is a forward air controller whose responsibility is to safely control CAS aircraft ordnance delivery. The FSCC reviews allocation of fixed-wing resources and subordinate requests for CAS support. The FSCC also plans for and coordinates future CAS requirements. The senior-level FSCC or equivalent presents a prioritized listing of requirements to the TACC. The TACC provides CAS sorties to Army forces based on the apportionment decision of the JFC while the DASC provides fast-reaction capability for immediate CAS requests. Aircrews receive the mission from either the ATO or the TACC. Requirements for effective CAS include air superiority, suppression of enemy air defenses (SEAD), target marking, favorable weather, flexible control, prompt response, aircrew, and terminal controller proficiency.

# Appendix C

## CAS Fundamentals

**Apportionment/allocation.** CAS is only one of the many missions of airpower. The JFC, through the JFACC balances the percentage of sorties among the various missions to achieve the campaign objectives. The JFC chooses this apportionment by using inputs from his various subordinate commanders and comparing the requirements to the availability of air assets. The Omnibus Agreement provides further guidance on the special airpower requirements of the Marine Corps' Marine Air Ground Task Force (MAGTF) concept. The JFACC takes the JFC apportionment decision and allocates the available CAS sorties to ground commanders. If the ground commander exhausts his allocated CAS sorties, he may request additional sorties. Conversely, he returns excess sorties to the JFACC for use on other missions.

**Communications.** FACs and other agencies pass detailed instructions on short notice to the aircrews. Specialized fire control, tactical air request, and tactical air direction nets are in place to plan, request, coordinate supporting arms, and direct aircraft. UHF and VHF channels are vulnerable to exploitation by the enemy, thus creating the potential for the disruption of CAS missions. Immediate missions are especially dependent on voice communication. The FSCCs at all echelons constantly monitor a special parallel communication net for fire support deconfliction and approval. The TACCs and FCCs use a "silence-is-consent" procedure that ensures minimum response time to fire support requests. A standard nine-line brief contains the information to complete a CAS mission.

**CAS categories.** There are two types of CAS requests: preplanned and immediate. Commanders use preplanned requests for anticipated CAS requirements. They allow detailed mission coordination and planning by the aircrews. Preplanned missions appear on the ATO and have an actual target, a location, and a target time. Ground commanders submit requests for preplanned CAS missions to FSCCs for evaluation, consolidation, and prioritization. The senior echelon FSCC makes the final consolidation and approves missions consistent with the CAS sortie allocation. The FSCC passes the missions to the TACC for execution. Preplanned CAS missions compete with other CAS missions for approval and placement on the ATO. Commanders at the battalion level or below use immediate CAS requests for unanticipated or urgent targets which do not appear on the ATO. FSCCs pass the request to the TACC for consideration. If approved, the TACC forwards the request to the Air Support Operations Center (ASOC) for execution. On immediate CAS missions, aircrews do not complete detailed mission planning and coordination before launching. The JFACC holds some aircraft on CAS alert (ground or air) to respond to immediate requests. The TACC has the option to divert aircraft on other missions.

**Normal aircraft procedures.** A pilot executing a CAS mission plans and flies a route to a predesignated contact point (CP). The pilot contacts the DASC or designated agency and receives further instructions. Pilots usually contact a FAC for final routing and coordination. Pilots fly CAS missions in a high or

reduced surface-to-air threat environment. Aircraft, artillery, or naval gunfire provide SEAD to reduce this threat. After completing the mission, the FAC passes BDA to the pilot who then flies through a return-to-force corridor to deconflict with other aircraft, supporting arms, and air defense engagement zones.

**Inflight briefing procedures.** Standard nine-line briefs are the joint format for passing CAS information. The brief includes heading, distance, target description, location, elevation, mark, friendly locations, egress instructions, and TOT. Combined operation briefings include the same information but can use different formats.

**Target acquisition.** Due to the tactical size, dynamic nature, and the necessity for specific target engagement, target acquisition can be the most difficult step of mission completion. Currently, visual recognition is the most common means of target acquisition.

**Aircraft losses.** The forward area of the battle area is usually heavily defended by air defense systems. This creates a high probability of aircraft loss or damage. Aircraft delivery parameters, multiple attacks, clearance to drop, and lack of SEAD all contribute to aircraft tactics that significantly increase CAS aircraft vulnerability.

**Ordnance.** Usually, weaponeers choose the specific ordnance for optimum effect on the target during preflight targeting meetings. CAS aircraft on alert for immediate missions may not be loaded with the best ordnance for the assigned target. As a result, the attack may be less effective than required.

**Clearance to drop.** Due to the close proximity of friendlies, the FAC clears each individual aircraft to drop ordnance. The FAC visually acquires the aircraft to ensure that it heads for the correct target. If the FAC fails to acquire the aircraft due to night, marginal weather, delivery profile, or small aircraft size, the FAC withholds the clearance. This necessitates multiple passes by the attacking aircraft, which considerably decreases its survivability.

**Target marking.** Targets are marked to improve visual acquisition. Laser designation and smoke are the most common means used to identify targets.

**Weather.** Poor weather conditions and night operations severely limit CAS effectiveness. Although the current use of night vision devices and sensor pods increase aircraft capabilities, significant limitations exist in marginal weather.

## Bibliography

***2025*** Concept No. 901165. "Personal Tactical Organizer." ***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept No. 901151. "Model Based Situation Database." ***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept No. 901131. "Real Time Battlefield Video." ***2025*** Concepts Database. Maxwell AFB Ala.: Air War College/***2025***, 1996.

***2025*** Concept No. 900913. "Virtual Battlefield Assessment Integrator." ***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025*** Concept, No. 901093. "Continuous Area Surveillance and Denial." ***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

***2025***, Concept No. 901175. "Holographic Image Projector." ***2025*** Concepts Database. Maxwell AFB, Ala.: Air War College/***2025***, 1996.

Aboulafia, Richard. "A Bomber Force Unrivaled." *Aviation Week & Space Technology* 144, no. 2 (8 January 1996).

Archambault, Raoul, and Thomas M. Dean. *Ending the Close Air Support Controversy*. Newport, R.I., 21 June 1991.

"Air Combat Command Operational Concept for the Joint Standoff Weapon (JSOW)." Draft, 28 May 1994.

AFM 1-1. *Basic Aerospace Doctrine of the USAF.* 2 vols., March 1992.

Buchanan, Thomas H. *The Tactical Air Control System: Its Evolution and Its Need for Battle Managers.* Airpower Research Institute Report No. AU-ARI-81-1. Maxwell AFB, Ala.: Air University Press, May 1987.

Correl, John T., ed. "More Data from Desert Storm." *Air Force Magazine* 79, no. 1 (January 1996).

Dornheim, Michael A. "New Sensors Show Two Paths to Reconnaissance." *Aviation Week & Space Technology* 143, no. 2 (10 July 1995).

Dunn, James C., and Donald L. Wiess. "B-2A Flight Test Progress Report." *Society of Experimental Test Pilots Symposium Proceedings*, 1995.

Essinger, Patrick J., ed. *Seabee Combat Handbook*. NAVEDTRA 10479-C2. Washington, D.C.: 1985.

FM 100-5. *Operations*, 1986.

FM 100-20. *Command and Employment of Airpower*, 21 July 1943.

FM 100-26. *The Air-Ground Operations System*, 1973.

FM 100-27. *USA/USAF Doctrine for Joint Airborne and Tactical Airlift Operations*, 1985.

Fulghum, David A. "ARPA Explores Unmanned Combat Aircraft Designs." *Aviation Week & Space Technology* 144, no. 9 (26 February 1996).

________. "Long Range Sensor Offers Options." *Aviation Week & Space Technology* 139, no. 2 (12 July 1993).

________. "Pentagon Cuts Field of JDAM Candidates." *Aviation Week & Space Technology* 140, no. 15 (18 April 1994).

Gourley, Scott R. "U.S. Army Warriors: 21st Century Equipment for 21st Century Missions." *Defense Electronics* 27, no. 1 (January 1995).

*Joint Force Air Component Commander (JFACC) Primer.* 2d ed, February 1994.

*Joint Pub 0-2. Unified Action Armed Forces (UNAAF)*, 1 December 1986.

*Joint Pub 3-0. Doctrine for Joint Operations*, February 1995.

Kiernan, Vincent. "The Eyes That Never Sleep." *New Scientist* 148, no. 2002 (4 November 1995).

"New Electronics Device Developed to Prevent Friendly Fire Incidents." *Defense Electronics* 27, no. 3 (3 March 1995).

*OH 5-4A. Close Air Support*, October 1985.

Sullivan, Gen Gordon R., and James M. Dubik. *Land Warfare in the 21st Century*. Carlisle Barracks, Pa.: Strategic Studies Institute, 1993.

Tirpak, John A. "Heavyweights for the New Strategy." *Air Force Magazine* 78, no. 10 (October 1995).

"Technology, Exploration and Exploitation Plan." Commandant's Warfighting Laboratory. December 1995. 4; on-line, Internet, January 1996, available from http://138.156.204.100/www/cwl/planch1.htm.

Treyz, Fred A., ed. "Force XXI, America's Army In the 21st Century." *Army Focus 1994*. Washington, D.C.: US Army Publication and Printing Command, September 1994.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century*, Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the attack volume, 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the munitions volume, 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the sensors volume, 15 December 1995.

# Counterair: The Cutting Edge

Col (Sel) Rick W. Lester
Lt Col Michael M. Miller
Comdr Steven M. Jacobsmeyer (USN)
Maj Stephen M. Tanous
Maj Jim C. Bigham, Jr.

## Executive Summary

This white paper examines the counterair mission in 2025—what it is, what the threats are, and how we counter them. In the broadest sense, the counterair mission will not change in the next 30 years. The basic premise of air superiority—neutralizing or destroying an adversary's ability to control the skies—will remain intact. This paper examines the counterair mission by first performing an analysis of three different trajectories. The first is an evolutionary trajectory based on projections of current and programmed capability. The second and third trajectories represent extremes—"anything but" approaches for conducting the counterair mission. The second trajectory is "anything but" inhabited aircraft, and the third is "anything but" aircraft at all—performing the counterair mission solely with surface and space-based systems. The results of this analysis will provide a basis of comparison for each.

Common themes emerge from all three trajectories. The primary theme is a requirement for near-real-time collection, processing, and distribution of information, or in some cases knowledge, to support the commander's assessment and reaction to a given situation. A comprehensive holographic display system is required to present the information to the commander. There also is a need for robust command, control, and communications networks distributed over commercial and military networks to pass this information. Finally, a synthesis of the three approaches will yield a system of systems—a counterair triad. The triad will be geared to handle a multiplicity of threats, from Cessna aircraft threatening the White House to uninhabited aerial vehicles attempting to monitor our operations, from Chinese-built stealth fighters in the Pacific to cruise missiles from Iran, or from terrorists with hand-held antiaircraft weapons to North Korean ballistic missiles. Inhabited vehicles provide flexibility where the fidelity of information available is limited or cut off, particularly in sensitive situations requiring definitive action as well as accountability. Uninhabited vehicles will provide a capability for rapid response using hypersonic, highly maneuverable, lethal and nonlethal application of force against an adversary's air forces. Space- and surface-based counterair forces can provide immediate precision strike against cruise missiles and intercontinental and theater ballistic missiles, as well as instant lethal and nonlethal force against forward air threats out of reach of available friendly air forces. A synthesis of the results of all three trajectories into a counterair triad will allow the strengths of each area to fill in the weaknesses of the other two, permitting a full range of nonlethal to lethal application of force against any adversary.

# Chapter 1

# Introduction

*The major thesis held by Trenchard and Mitchell, as well as Seversky, was that command of the air is of first priority to any military success in war.*

—Maj Gen Dale O. Smith

Airpower is the cutting edge of the sword of the Republic, and upon that sword the Republic will stand or fall—a situation that will exist in 2025, just as it exists today. This paper describes the counterair operational world of 2025. The world of 2025 will be different from the world of 1995. This is a given; the question is: how different? Part of the approach of the 2025 program is that there be no surprises. The approach taken here is to first perform an analysis of how the counterair mission could be accomplished using the "anything but" construct. This analysis looks at the counterair problem from several different perspectives. The first perspective is a projection looking out from 1996 to 2025 based on what we know today. The second and third perspectives are extremes, used to facilitate analysis of the problem. The second perspective examines counterair using anything but inhabited aircraft. The third perspective includes anything but air-breathing aircraft.

The next part of the analysis requires a recognition of where technology is headed and where the Air Force leadership is placing its emphasis. A review of *New World Vistas* demonstrates an emphasis on reduction in USAF spending on specialized systems for common needs (such as communications), a view towards uninhabited air vehicles (UAV), and increased reliance on command, control, communications, computers, and intelligence ($C^4I$) and space.[1] As commercial enterprises outstrip the ability of the military to fund advanced research and technology initiatives, it behooves the US armed forces to take advantage of their efforts rather than fund separate "stovepipe" military systems.

*Air Force Executive Guidance*, December 95 Update, focuses on "effective planning for future alternatives."[2] It provides a thumbnail sketch of the environment and threat, as well as specific planning guidance. It then describes offensive airborne vehicles and weapons of mass destruction (WMD) as the most direct threat to US security. The key assumptions drawn from it are an increasing air-breathing threat, including cruise and theater ballistic missiles; an increasing requirement for nontraditional defense systems, such as high-power microwave and lasers against attacking aircraft; and a continuing requirement to suppress enemy air defenses as a prerequisite for air superiority. The guidance that falls from these assumptions is consistent; there is a need to detect, locate, identify, engage, and destroy targets on the surface (both fixed and mobile) and in the air, as well as to ensure onboard threat warning and self-protection systems for aircraft of all air forces.

Finally, a review of the threat environment puts proposed capabilities into proper context. A briefing given by the special assistant to the chief of staff for long-range planning (HQ USAF/LR) to the Defense Science Board in March 1996 describes three types of future adversaries. The first type is a regional adversary, who is expected to challenge the US in its geographic area (such as Iraq or North Korea). The second type is a peer competitor, which is viewed as

likely to emerge in the long term. A peer competitor could be a nation or group of nations with broad-based military power projection capability, able to threaten US or allied interests in more than one region of the world, and could include a resurgent Russia or emergent China. The third possibility is a niche competitor, including nonnation/nonstate actors capable of acting against US interests (i.e., terrorists or drug cartels).[3]

Combining these views results in three different trajectories, each with a different outcome for how the counterair mission could be conducted in 2025. The first is the evolutionary trajectory. An extrapolation from today in terms of development and modernization programs, this trajectory assumes a world of continuing technological advancement, relatively constant US defense spending, and world players in the same relative positions of strength. Air superiority and the counterair mission will be dominated by existing airframes and those already budgeted or in development. UAVs and space assets will augment these to accommodate smaller air forces relying on power projection from the continental United States (CONUS), aircraft carriers, and a select few major overseas bases.

The second is the "penurious robophile"—cheap robot-lover—trajectory. This assumes a significant reduction of defense spending, coupled with significant advances in technology and its application. An American worldview focused internally but still concerned about external threats drives the air superiority mission towards a reliance on awareness and a reactive standoff capability, representing air forces in being—the strength of the force is in its capabilities, not its size. This cut in spending, reliance on technology, and reluctance to expose US armed forces personnel to risk leads to a primarily UAV counterair capability.

In this trio of possible paths the counterair mission might follow, the last is the virtual trajectory. This trajectory assumes a globally minded United States with a surplus of technology and a budget to back it up. It represents the ultimate in virtual presence, virtual power. It is a ubiquitous space-based capability that includes not only force enhancement capabilities but force application, complemented by surface-based assets for those hard-to-reach, hard-to-kill targets or those evading the space-based assets. This capability allows all the functions listed in the *Executive Guidance* (detect, locate, identify, engage, and destroy targets) to be performed almost instantly.

This white paper reviews each approach with a critical eye towards the goal of no surprises. The triclinic of these trajectories will result in a synthesis of capabilities designed to provide assured air superiority in 2025.

This paper assesses the future counterair mission using the following organization: (1) to define the counterair mission and the focus of this white paper; (2) to develop the assumptions, required capabilities, systems, enabling technologies, and concepts of operations in each of the three trajectories; and (3) to recommend a counterair capability based on a review of these results in the context of ensuring no surprises and assured air superiority and develop a concept of operations for employment by 2025.

## Counterair Defined

*If we lose the war in the air, we lose the war and lose it quickly.*

—Field Marshal Bernard L. Montgomery

Counterair is a mission that currently falls under the role of aerospace control. The focus of this white paper is limited to counterair (not counterspace) operations; however, the future is bringing with it a fusion of air and space capabilities that will increasingly blur the distinctions between counterair and counterspace operations. Aerospace control permits aerospace and surface forces to operate freely while denying access to the aerospace by the enemy.

Counterair is the enabler that makes this possible. This is true today and it will be true in 2025. The counterair world of 2025 will be a smaller world where the Atlantic and Pacific Oceans will not provide the obstacles to offensive/defensive air operations they do today. The definitions for counterair and the counterair missions follow.

*Counterair* is a term for operations conducted to attain and maintain a desired degree of air superiority by the destruction or neutralization of enemy air forces. Both air offensive and air defensive actions are involved. The former range throughout enemy territory and are generally conducted at the initiative of the friendly forces. The latter are conducted near to or over friendly territory and are generally reactive to the initiative of the enemy air forces. For example, an F-22 launching an antisatellite missile at a space-based laser attacking friendly air forces would be a counterspace sortie. On the other hand, an F-22 taking defensive measures against a space-based platform is included in the counterair arena. As a guideline, action taken against space assets by air assets in a defensive response is included in the counterair mission area, while preplanned missions against space assets are counterspace missions. Additionally, in 2025, countering the cruise missile and theater ballistic missile (TBM) threat will be a part of both the offensive and defensive counterair mission.

*Offensive counterair operations* are operations mounted to destroy, disrupt, or limit airpower as close to its source as possible. While suppression of enemy air defenses (SEAD) is clearly in this category, the tactics and weapons to destroy, disrupt, or disable the enemy air defenses fall under the categories of tactical/strategic attack.

*Defensive counterair operations* provide the protection of assets from air attack through both direct defense and destruction of the enemy's air attack capacity from the air.

## Why Counterair?

*It is our principal responsibility to provide the umbrella under which US and multinational forces may operate. Our success in military operations in the future, wherever or whenever they might be, will depend on how successful we are in this area.*

—Secretary of the Air Force
Dr Sheila J. Widnall

A common question, asked since the birth of airpower, is, Why is air superiority important? The answer lies in examining the purpose for the use of air forces. When the enemy is engaged in insurgency, without an organized air force, friendly air forces seek to minimize the fog of war through the use of reconnaissance and surveillance assets, limit the insurgent's freedom of action through interdiction, or reduce the enemy's ability to mount sustained operations through strategic attack. Successful prosecution of the counterair mission reduces the risk to friendly air and surface forces while increasing the risk to enemy operations. Suppression of enemy air defenses (even as simple as the shoulder-launched weapons that today are available to even the most rudimentary terrorist organization) becomes a deciding factor in the application of airpower.

Against a heavier, more conventional foe, enemy air forces (inhabited and uninhabited) become a threat to friendly forces—air, ground, and naval. In this instance, the more familiar notions of air superiority take over. The cycle comes full circle against a foe who can, but chooses not to use airpower, and instead employs cruise missiles, directed energy weapons, or more crude but equally effective measures such as radio frequency (RF) jammers or highly accurate antiaircraft artillery (AAA). In every instance, air superiority is essential.

While it may be true that in each case the success of the counterair mission may not be the sole deciding factor, it will at a minimum be the enabler that allows the

success of the other elements of US military power to come to the fore. This alone is sufficient reason to examine the counterair mission in 2025.

## Notes

1. *New World Vistas* distinguishes between uninhabited reconnaissance aerial vehicles (URAV) and uninhabited combat aerial vehicles (UCAV) for combat and noncombat UAVs. See *New World Vistas: Air and Space Power for the 21st Century*, summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 8, 11.

2. *Air Force Executive Guidance*, December 1995 update, 4.

3. Briefing, HQ USAF/LR to the Defense Science Board, subject: "Air and Space Power Framework for Strategy Development," 19 March 1996.

## Chapter 2

# The Evolutionary Trajectory: The Fighter Pilot—Here to Stay?

*The most important thing to have is a flexible approach. . . . The truth is no one knows exactly what air fighting will be in the future. We can't say anything will stay as it is, but we also can't be sure the future will conform to particular theories, which so often, between the wars, have proved wrong.*

—Brig Gen Robin Olds

The first trajectory evaluated is the *evolutionary trajectory*, an extrapolation of where the US is today. Assuming a world of continuing technological advancement, relatively constant US defense spending, and world players in the same relative positions of strength, air superiority and the counterair mission will be dominated by existing airframes and those already budgeted or in development. UAVs and space assets will augment these to accommodate smaller air forces relying on power projection from CONUS, aircraft carriers, and a select few major overseas bases.

*If a man's trust is in a robot that will go around the earth of its own volition and utterly destroy even the largest cities on impact, he is still pitiably vulnerable to the enemy who appears on his doorstep, equipped and willing to cut his throat with a penknife, or beat him to death with a cobblestone. It is well to remember two things: no weapon is absolute, and the second of even greater import—no weapon, whose potential is once recognized as of any degree of value, ever becomes obsolete.*

—J. M. Cameron

While uninhabited aerial vehicles will be widespread in 2025, the inhabited vehicle will be the backbone of air forces around the world. Space assets will have active and passive antiaircraft capabilities. Likewise, aircraft will have antisatellite active/passive capabilities. Multiple detection technologies will abound, with radar remaining as the primary active detection medium. Air-to-air/space-to-air/air-to-space combat operations will be increasingly lethal. While the current generation of air-to-air missiles like the AIM 9, Python 4, and the advanced medium range air-to-air missile (AMRAAM) have demonstrated high probability of kill ($P_K$), in 2025 missiles will be even better—smaller, faster, and more accurate. The surface-to-air missiles (SAM) and space-based weapons (SBW) can also be expected to exhibit similar increases in lethality.

In spite of technological advances, dogfights likely will still occur in 2025. Fighters in 2025 will still have a "gun." The lessons learned from development of the F-4 will still apply. In the 1950s the development of air-to-air missile technology negated the gun requirement for the F-4. By 1965 lessons learned in Vietnam necessitated a gun retrofit for the F-4C/D; the F-4E was designed with an internal gun. Every multirole fighter built or designed since, including the F-22, has included a gun. The counterair mission will require a variety of weapons to use against the entire spectrum of threats and available countermeasures. The gun will remain a lethal weapon when everything is electronically jammed or laser blinded.[1] This advanced gun may have the capability to fire solid projectiles and/or directed energy beams. Also, if history is any indicator, the multistaged improvement (MSIP) F-22 will still be operational, and possibly upgraded versions of the F-15 as well.

## Counterair Requirements

*We're not in the business of being defensive when we engage. We want to take the fight to the other guy and we are going to dominate his airspace. We will operate in it, and he will not.*

—Gen Ronald R. Fogleman

The aircraft force mix of 2025 will evolve from the current developmental programs, including the F-22 and derivatives, the joint strike fighter (JSF), and a number of UAVs, to both support inhabited vehicles and to operate independently. The F-22 derivatives may include a Wild Weasel platform that will be able to target both radio frequency (RF)-guided surface-to-air missiles (SAM) and directed energy antiaircraft weapons. UAVs will be used predominately to engage high-threat antiaircraft weapons and to provide active sensors for inhabited vehicles that will rely on passive sensors for the majority of their situational awareness.

Sensors and the data they provide will be widely distributed to provide maximum situational awareness. Fighter-mounted sensors should supply information to companion aircraft as often as they provide information to their bearer. Detection and identification probabilities will increase rapidly with sensor diversity and the false-alarm probability and error rates will decrease correspondingly. Uninhabited combat aerial vehicles (UCAV) should provide active sensors that work cooperatively with passive sensors on low observable (LO)-inhabited aircraft. Technologies such as high bandwidth, secure communication for satellite, and aircraft cross and downlink must be developed.

## System Descriptions

The F-22 will be the only new fighter available to the US in the next decade. The joint strike fighter should appear after that to replace most current US fighter aircraft. By the time the F-22 and JSF appear, new technologies will be available to enhance their performance, but both aircraft are being designed using extant technologies. These aircraft will not produce a revolutionary change in the way air combat is waged. They represent an evolutionary change in the capabilities of aircraft. As 2025 comes to pass, the US will still have the requirement to control the air over enemy territory. This capability will come from the planned aircraft for the first part of the twenty-first century such as the F-22 and JSF, but also a whole new breed of uninhabited vehicles.

The twenty-first century, and the threats that accompany it, will require the capability to project airpower over a wide area of responsibility relative to today. This trajectory employs a mix of inhabited and uninhabited vehicles to accomplish the counterair mission. The inhabited vehicles will be a mix of upgraded F-22s and JSF aircraft. The uninhabited vehicles will be a whole new family of combat aircraft that will both support the inhabited vehicles and carry out some missions autonomously. If technologies develop as some believe, the concept of a "FotoFighter" as discussed in *New World Vistas* could be a reality in small numbers, or as a prototype. These aircraft would use large arrays of diode lasers to communicate, designate, and execute thermal kills of targets.[2]

Both inhabited and uninhabited vehicles will have a requirement to detect, identify, and target all types of airborne targets. This will require a combination of improved situational awareness, sensor capability, and lethal weapons. Significant effort will be required to expand beyond the current sensor suites forecast to allow the pilot to correctly identify threats, even if they are stealthy and their sensors are not actively emitting. This capability will increase survivability when the US is outnumbered in future air battles.

### Situational Awareness

The cockpit in 2025 should be linked to virtually every available source with high-bandwidth communications to ensure the

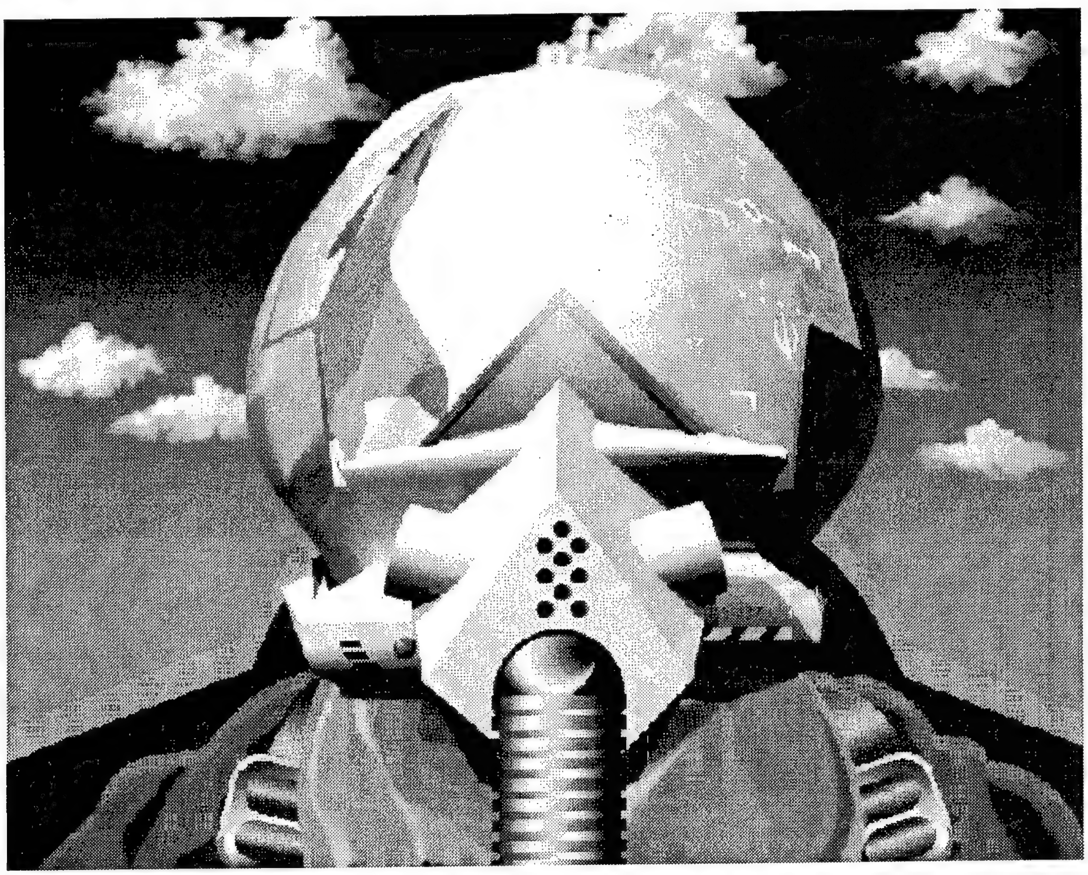
highest degree of situational awareness.[3] Satellite surveillance networks, sea-based and land-based sites, and mobile platforms in the air and on the battlefield will play vital roles in providing the uplink and downlink of targeting information, individual engagement status, and battle space management directly to the operator.[4]

Onboard computers will correlate all information and display it to the aircrew in a helmet-mounted display (HMD) (fig. 2-1).[5] Visual presentations will also be displayed using long-range reconnaissance platforms and missile status uplinks. Cockpits will be fully compatible with night and all-weather operations. Fighter-mounted sensors will provide updates to companion aircraft (and vice versa) as often as they provide updates to their bearer.[6]

**Detection and Acquisition**

Airborne detection of adversary aircraft will be increasingly easy in 2025. Cutting edge technology in 1996 will be commonly available and widely dispersed. Effective airpower hinges on early detection and employment of weapons. Detection techniques will incorporate high-confidence, real-time situational awareness (SA) with highly diversified, multisensor detection capabilities and very lethal air-to-air weapons to ensure first launch, first kill and survivability of the launching platform.[7]

It is imperative that target detection and acquisition (hereafter jointly referred to as targeting) occur at the longest possible ranges. Identification of the detected vehicles at the earliest possible time will be



**Source:** http://www.thomson.com:9966/janes/jpictl.html, Geoff Fowler Media Graphics © 1995.

**Figure 2-1. 360-Degree Helmet-Mounted Display**

critical to survival of the launching platform. Precision targeting will be possible using linked information from both surveillance and reconnaissance satellites and early warning aircraft correlated to that from onboard sensors.[8] Laser detection and ranging (LADAR), coupled with advanced global positioning system (GPS) inputs, will provide the longest range detection probability in clear air mass.[9] Radar of one form or another will still provide the longest range detection in adverse weather. Artificial intelligence will aid the aircrew by filtering through and sorting a plethora of linked information on possible targets.[10]

### Weapons

To take advantage of complete SA, as well as first detection and acquisition, airborne weapons must be flexible, long-range, smart, and extremely lethal in all quadrants. Only a single type of air-to-air missile, possessing the capabilities necessary to ensure destruction of adversary aircraft, is necessary. The missile must be common to all US armed forces, with ordnance personnel from any service able to perform necessary maintenance. The endearing feature of this missile will be its ability, once launched, to perform the entire intercept independent of the launching platform.

Prelaunch information will be input to the missile, either from the aircraft or from external sensors, at increased speeds, proportional to an increased onboard computability. Postlaunch updates, if necessary, will be a combination of inputs from the launch platform and/or the same targeting sensors linked to the aircraft via secure low probability of intercept (LPI) datalink. Conversely, missile status will be linked from the weapon to targeting sensors and the launching platform throughout the engagement, including endgame battle damage assessment (BDA) to enhance SA.[11]

At launch input, the weapon will compute an intercept trajectory and fall from the aircraft. Using reactive jets, the missile will turn to the correct heading and then begin the boost phase of flight. Active detection capability inherent in the missile will compare data to all available outside sources to ensure precision intercept to the correct target. Autonomous target acquisition will occur and advanced guidance laws, coupled with guidance integrated fusing, will assure intercept and kill. Postlaunch missile-to-cockpit status will allow the aircrew to determine subsequent courses of action regarding the target in question.[12]

Dependent upon the range to target at launch, the missile will move from the boosted phase flight to a sustained flight stage. Optimum altitude and speed for the missile will be computed based on target data.[13] This will give the missile the greatest potential flexibility during midcourse and terminal phases.

Precision GPS-derived location will be a primary guidance source during the weapon's entire time of flight. During the terminal phase of the intercept, the missile will incorporate the GPS guidance with precision onboard targeting technology to effect missile-target intercept. Terminal tracking and guidance may employ a combination of LADAR, infrared (IR), magnetic anomaly detection (MAD), jet engine modulation (JEM), photographic, and acoustic sensors, dependent upon weather and atmospheric conditions.[14] It is important to note that we expect that multimode seekers will be required based on expected countermeasure proliferation. Multiple warhead missiles will be possible with guidance to each warhead in the terminal phase.[15]

### Countermeasures and Countercountermeasures

Survival in a hostile integrated air defense system will be essential. Survival will depend on avoiding detection to accentuate the advantage of surprise in a tactical environment. Enemy detection capabilities will have increased to the point where both active and passive stealth techniques will be necessary. Other

countermeasures should include both expendables and nonexpendables, as well as redundancy and reconfigurability of the air vehicle. Expendable countermeasures will include micro-UAVs that actively engage inbound threats to the vehicle it is protecting. If the vehicle is detected, it will have to recognize that detection and then be able to precisely locate and identify what has detected it so that that sensor can be deceived, jammed, or targeted.[16]

## Enabling Technologies

Active radio frequency and passive infrared stealth capabilities will be the highest payoff technology development for the evolutionary trajectory.[17] Active stealth capability should allow the US to develop techniques that will provide survivability and lethality to more platforms. The expense of developing passive stealth beyond current capabilities will increase exponentially but will not provide backwards compatibility to older platforms that active techniques might provide. Some of the active stealth concepts developed might include active cloaking film using nanotechnology-based film of micro-robots that vary their color and reflectivity to make an object "invisible" and "paint" with electro-optic materials that adopt a range of colors depending on the voltage applied.[18] These materials could be used to effectively provide active stealth in a particular bandwidth. No single system is envisioned which could provide a cloaking capability across the electromagnetic spectrum.

The fusion of multispectral sensors from different platforms will provide the next leap of capability in 2025 (fig. 2-2). Air vehicles will require the exploitation of offboard information using a high-bandwidth, secure datalink to increase SA and allow real-time targeting. Sharing of the offboard information will be enhanced by artificial intelligence-based cooperation and distribution of mission responsibilities between platforms.[19] A distributed satellite system for surveillance and datalink to aircraft will allow the information to be shared throughout the theater of operations, providing real-time command and control.[20]

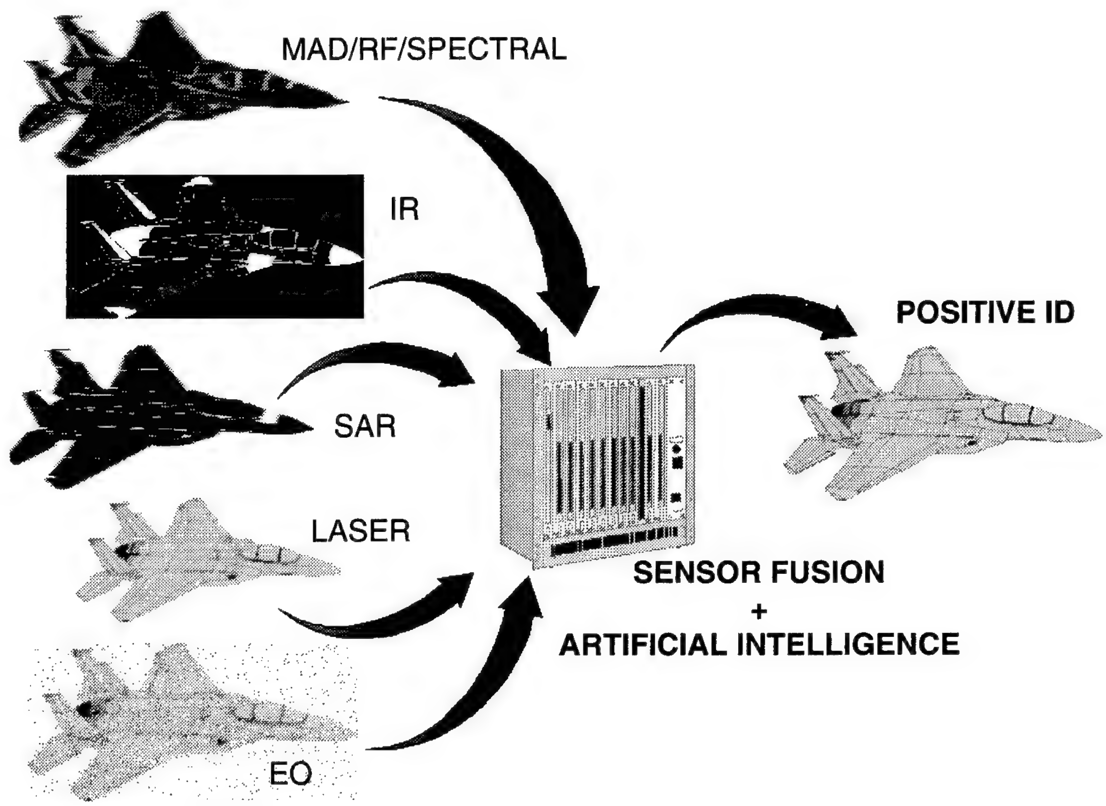
It is essential that the sensor technology continue to be developed to provide capability against a growing countermeasure proliferation. These technologies include integrated sensors and conformal apertures with open system architectures, cooperative and distributed electronically scanned arrays, and multispectral, multimode seeker heads.[21]

Advanced identification friend or foe (IFF) capability will need to be developed to allow adversary platforms to be targeted with confidence at long range for survivability of the launch platform. Problems exist in current IFF systems that prevent long-range launch of long- and medium-range weapons at optimum ranges. These must be overcome to both negate the possibilities for fratricide and allow effective use of longer range weapons. One option could include the use of LADAR IFF. LADAR would provide 3-D mapping of the target to perform identification (ID).[22] The use of sensor fusion across platforms will also help in this endeavor.

After adversary platforms have been detected and identified, the platforms have to be neutralized as a threat. It is imperative that weapons technologies remain lethal in an environment of increasingly sophisticated countermeasures. Advanced munitions and missiles with multispectral and multimode seeker heads will be a necessity. Warhead development that includes nonlethal high-power microwaves will provide the capability to destroy or neutralize the electronics of targeted aircraft or systems.

## Concept of Operations

Air superiority fighters will operate in conjunction with UCAVs using active sensors and/or weapons appropriate to the mission and will communicate through a worldwide communications data network. A worldwide joint tactical information display system (JTIDS) will provide high-resolution data to both the commanders and the aircraft actually in combat. Space systems




**Source:** Clipart elements from Federal ClipArt © 1995 with courtesy from One Mile Up, Inc., and Microsoft Clipart Gallery © 1995 with courtesy from Microsoft Corp.

**Figure 2-2. Sensor Fusion and Target ID**

will provide the surveillance picture to the network. The artificial intelligence (AI) capability in the aircraft and drones will use both onboard and offboard inputs to give recommendations for tasks such as targeting, a-pole, and ordnance selection.[23] This worldwide data network will result in a flattened hierarchy for command and control. The potential threats and the mission to be accomplished will determine the mix of inhabited fighters and UCAVs in a force package.

Once the inhabited fighters and UCAVs have established their defensive combat air patrol (CAP) or offensive sweep, they will use a combination of onboard active and passive sensors and the available data linked information to search their area of responsibility. The AI software in the avionics will fuse the data from multiple sensors, both on and offboard the vehicle, to detect and identify air vehicles (bombers, fighters, cruise missiles, etc.) and develop situational awareness displays for the pilots of the fighters or UCAVs. The decision to engage or avoid the threats will be made and communicated directly to the entire chain of command via the JTIDS link.

If the decision to engage is made, the fighter (or UCAV) will attempt to employ weapons at maximum range to increase survivability. The weapon employed will depend on the current weather conditions and countermeasures employed by the adversary. Ideally, a directed-energy weapon from a FotoFighter could be employed against numerous threats in a very small time period. Since the F-22 and JSF fighters

will still be limited to missiles previously discussed in this chapter, the engagement may occur at closer ranges due to late identification of the threat or because longer range weapons may be defeated by countermeasures. Very strict rules of engagement (ROE) could also lead to close-in visual engagements. In either case, the requirement for a close-range weapon appears inescapable. The weapons employed at close range could vary from high power microwave (HPM) to "bullets" from an advanced gun.

Once the engagement is finished, the fighters will return to their assigned area of responsibility or refuel to continue the mission. If the mission objective has been achieved, or if fuel and weapons are not sufficient to continue, the fighters and the UCAVs will return to base. The results of the engagements and significant intelligence information will be passed through data link to update the command and control system. This type scenario will be played again with multiple flights of air vehicles, both inhabited and uninhabited, throughout the area of responsibility for the particular joint force aerospace component commander (JFACC). The force mix and tactics involved will be determined by the mission objective and the perceived threat.

## Summary

The capability described above is based on the assumptions that technological advancement between now and 2025 will be evolutionary, and that inhabited vehicles are the dominant means of maintaining air superiority. Since the advent of the counterair mission, we have seen under what circumstances conventional air forces will prevail—typically when the adversary presents a similar capability, such as World War II, Korea, or the Gulf War. There have also been situations, such as in Rwanda or Somalia, where counterair capabilities have played a lesser role. From this it can be concluded that evolutionary counterair capabilities are best suited to a peer or regional competitor, vice a niche competitor during an insurgency or guerrilla war. This is primarily because conventional counterair forces, as we know them today, have limited nonlethal capabilities. An additional limitation is the fragility of inhabited aircraft systems. The high cost of individual airframes, the cost of training pilots, and the requirement for forward basing in a potential threat area may make the American public too risk-averse to the employment of airpower under even the most compelling circumstances.

However, these are more than counterbalanced by the feasibility of these systems; and survivability of these systems will increase as more complex countermeasures are employed. The passive stealth features of the F-22 and JSF will be a significant improvement over the F-117. The next generation of active countermeasures need not be tied to the airframe technology. Indeed, as nanovehicles become the norm, they will find increasing use providing countermeasures in a hostile air-to-air environment. UAVs could also provide an active countermeasures screen to allow inhabited vehicles with passive countermeasures to penetrate enemy air defenses and engage enemy air forces directly. Upgrades to the present airborne laser program will support the targeting of smaller, more advanced counterair threats such as ballistic and cruise missiles.

Finally, one of the most important reasons for maintaining inhabited air forces will be accountability. In 2025, many of the competitors the US is likely to face will be regional competitors, whose inventories will be little different from what they have today.[24] In circumstances where the nature, or more likely the intent, of enemy air forces is not known, a higher level of fidelity—that provided by the pilot—will be necessary to discern the true air threat to the US or its allies. The situational response to many of the circumstances involving a regional or niche adversary in 2025 requires the hands-on accountability that is only possible

with inhabited aircraft. In addition, most high-technology weapons such as lasers or HPM, are not recallable; once engaged, the target is permanently affected to the degree the engagement has progressed before it is terminated. There will also be situations where strict ROE demands a pilot on-scene to make a real-time determination of the actual threat presented. The international political and practical ramifications of an accidental shootdown by uninhabited US systems of either nonbelligerents, or enemy forces whose intent was in question would be significant; it would probably dwarf the response of the international community to situations such as the shootdown of civilian aircraft by the Cuban air force in February 1996. The bottom line is that warfare is still an engagement between two reactive entities, and the instincts and finesse of the pilot will be required to gauge the situation, either to defend the US or prevent an international incident.

**Notes**

1. David R. Mets, *Checking Six Is Not Enough: The Evolution and Future of Air Superiority Armament,* CADRE Paper Special Series: The Future of the Air Force, no. AU-ARI-CPSS-91-14 (Maxwell AFB, Ala.: Air University Press, April 1992), 34.

2. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the directed energy volume, 15 December 1995), viii.

3. ***2025*** concept, no. 900619, "Panoramic Night Vision Goggles," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

4. Headquarters Air Force Materiel Command, *FY96 Avionics Technology Area Plan,* 1995, 18.

5. ***2025*** concept, no. 900365, "Sensor Cockpit," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

6. *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 11.

7. ***2025*** concepts, no. 900202, "Space-based Special Operations Forces," no. 900317, "Tactical Information Display Helmet," and no. 900364, "Bionic Eye," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

8. *New World Vistas,* summary volume, 20.

9. ***2025*** concept, no. 200014, "Molecular Inertial Navigation Sensor," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

10. *FY96 Avionics Technology Area Plan,* 18-19.

11. ***2025*** concepts, no. 900405, "Weapon Health Monitoring"; and no. 900675, "Ordnance Enroute Reporting," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

12. Ibid.

13. ***2025*** concepts, no. 900359, "Air-to-Air Missile Interdiction"; no. 900554, "Adaptive Munitions"; and no. 900555, "Sensor-to-warhead Operations," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

14. ***2025*** concepts, no. 900211, "LADAR Identification Friend or Foe"; no. 900508, "Magnetic Detection of Aircraft"; no. 900239, "Space-based Missiles with Photo Warheads"; and no. 900392, "Acoustic Weapon," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); *FY96 Conventional Weapons Technology Area Plan* (Headquarters Air Force Materiel Command, 1995), 7.

15. ***2025*** concepts, no. 900288, "Swarms of Micro-Machines"; and no. 900676, "Defense of Missile-Delivered, Multiple Conventional Warheads," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

16. *FY96 Avionics Technology Area Plan,* 11-13.

17. *New World Vistas,* summary volume, 60.

18. ***2025*** concepts, no. 900605, "Active Cloaking Film/'Paint'" and no. 900573, "Dielectric Materials For Stealth," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

19. "Cooperative Air-to-Air/Air-to-Ground Engagements-Distributive Fire Control," *Technology Initiatives Game 95 (Systems Handbook),* 18-22 September 1995, 20-1.

20. *New World Vistas,* summary volume, 20, 43.

21. "Cooperative ESA Jamming," *Technology Initiatives Game 95 (Systems Handbook),* 18-22 September 1995, 21-1.

22. ***2025*** concept, no. 900211, "LADAR Identification Friend or Foe," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

23. ***2025*** concept, no. 900414, "Artificial Intelligence: A New Aircrew Member in Tomorrow's Combat" and no. 900550, "Personal Digital Assistant," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

24. Col Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala.: Air University Press, January 1996), 94.

# Chapter 3

## The Penurious Robophile Trajectory: Pilots—the Rarest Breed

*Why can't they buy just one airplane and take turns flying it?*

—Calvin Coolidge

*No system exists which can provide continuous all-weather coverage of worldwide targets. . . . To meet the above requirements, the Joint Staff has identified an urgent need for the capability of an Endurance Unmanned Aerial Vehicle (UAV) System.*

—Dr John M. Deutch, Under Secretary of Defense (Acquisition and Technology) July 1993

The road to 2025 may be sown with domestic strife and the propensity for the US to look inwards at its own problems. If so, US interest in world issues and debates would be greatly reduced, while concern for threats to US security from foreign countries or groups would be only as real as the threat. The same domestic problems driving this inward emphasis would drive consistently low defense budgets and interest. Technology would continue its near exponential rate of climb, but with an emphasis on domestic uses. The successful use of UAVs in the Gulf War in 1991 and in Bosnia in 1995–96 might motivate the US to accelerate the development of more advanced, multipurpose UAVs.[1] This technology offers more potential for weapon system performance at apparently lower costs. At the same time, UAVs "serendipitously accommodate the probable inexorable trend of American society who are more and more expecting no losses during US military operations."[2]

Although defense budgets and interest by the average citizen may be low, technologies applied to commercial communications and other areas such as electronics and materials would migrate to military applications as a leverage against lower budgets. Sensors and propulsion systems would continue to improve at similar rates. A more advanced and jam resistant global positioning system (GPS) constellation might replace the stage 2R satellites deployed between 2000–2010.[3] The level and sophistication of enemy air defenses might grow with technological advances to the point where inhabited systems must accept much higher risks for missions over enemy territory. At the same time, the cost of survivable inhabited systems would grow exponentially, making the development and fielding of these systems economically impossible.[4] In such a world, the joint service Defense Airborne Reconnaissance Office (DARO), formed in 1993 to manage the UAV program, not only survives early budget challenges and interservice rivalries, but grows in scope and responsibility.[5] By the year 2010, DARO might be responsible for the development of all UAV systems regardless of mission. In an effort to maximize smaller defense budgets and maintain consistency with the unsupportable expense of inhabited weapon systems and the sophistication of air defenses, civilian and enlisted pilots are recruited to "fly" the uninhabited air forces of 2025.[6] A fleet of multipurpose UAVs would then replace the aging fleet of F-15s. The F-22, joint strike fighter, and other

proposed inhabited fighter and attack aircraft programs would all be canceled due to escalating development costs and the public perception of no real threat. Support and airlift aircraft, maintaining orbits far from potential air defenses, are available for the launch, retrieval, and rearming of UAVs. In the world of 2025, the fighter pilot of old is indeed rare.

## Counterair Requirements

As mentioned previously, enemy air defenses have grown more sophisticated with technology. This requires the ability to detect, locate, identify, engage, and destroy fixed and mobile surface and air targets anywhere in the world on short notice. A limited overseas presence and a complex political environment demand power projection with greater precision, less risk, and more effectiveness.[7] Therefore, the uninhabited counterair force of 2025 must have the ability to deploy from CONUS, strike a target anywhere in the world, and return to a friendly base in CONUS, in the air, or at sea. These operations require a mix of autonomous and controlled flight missions. Finally, nontraditional defenses against aircraft, like high-powered microwaves, and an increased air-breathing threat, especially cruise missiles, will put a premium on a counterair force mix capable of meeting both the offensive and defensive counterair requirements of 2025.

## System Descriptions

The UAV force mix of 2025 evolves from development efforts in the late 1980s and early 1990s, and draws on the combat experience of Bosnia in 1995–96. Stealthy, high-flying, very long-range systems use modular sensor and weapon bays and air or surface launch and recovery for optimal mission flexibility. The Tier 2 Predator, Tier 2 Plus, and Tier 3 DarkStar UAVs fielded in the 1990s were the first systems to demonstrate high-altitude, long-range, and stealth capabilities, respectively, using commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technology.[8] The counterair system of 2025 combines the attributes of each of these systems into a single, stealthy system capable of unrefueled global range and the ability to operate from low, terrain-following altitudes to altitudes over 100,000 feet.

The multipurpose UAV of 2025 has an advanced turbofan engine, is structured almost entirely of composites, and has a minimum payload of 2,000 pounds.[9] If technology development permits, a UAV capable of transitioning from air-breathing propulsion to hypersonic capability and back again provides even longer range, higher altitude, more rapid reaction, double digit mach speed, and the enhanced survivability derived from these advancements.[10] Advances in materials and sensors provide for embedded sensors (smart skins) for 360-degree awareness and communications.[11] Reconfigurable control surfaces (smart structures) optimize range and performance while minimizing radar cross section.[12]

In addition, active stealth systems will eliminate other detection vulnerabilities.[13] Increasing maneuverability beyond human tolerance, plus or minus 12 Gs or more, enhances survivability; increasing to plus 20 to 40 Gs greatly enhances missile avoidance in the endgame.[14] In addition, advanced defensive avionics use active and passive systems, including mini-UAV decoys and other expendables.[15] Modular sensor suites and weapon bays provide snap-in and snap-out mission customization, keeping unit fly-away cost for the basic air vehicle to the equivalent of today's cost of $10 million.[16]

### Applications

In the year 2025, intelligent signal and data processing and secure, redundant data links for control and intervehicle information sharing are standard.[17] The multipurpose UAV will employ the latest synthetic aperture radar (SAR), bistatic radar, infrared (IR), and electro-optical (EO) target tracking

capability, target illuminators, and jam-resistant, low probability of intercept (LPI) communications and data links to perform any of the envisioned counterair missions.[18]

The air tasking order (ATO) of 2025 will be automatically deconflicted by using surface-, air-, and space-based sensors to provide a synergistic effect for netted systems. Advances in artificial intelligence, computing speed, and secure communications links will make real-time ATO deconfliction and tasking a reality.[19] The joint forces commander of 2025 will display situational awareness and battle management information in the holographic war room with the assistance of UAVs while directing other UAVs to fight the counterair battle.

**Weapons**

The multipurpose UAV will employ the latest in advanced weapons for air-to-air and air-to-ground attack. The advent of very small, very smart bombs and missiles will optimize payload capacity.[20] Explosives with 10 times the destructive force for the same weight will make these sorties 10 times more effective than today.[21] Advanced GPS receivers embedded in individual powered or unpowered weapons provide fire-and-forget capability without the need for laser illumination from other platforms or sources.[22] Smart fuses will enhance hard target kill, while the launch UAV or another UAV in the mission package provides real-time BDA via satellite uplink.[23] Advanced air-to-air weapons will use vectored thrust for optimal turn performance. Distributed satellites and advanced GPS provide worldwide, jam-resistant, low probability of intercept command, control, communications, navigation, and pinpoint weapons delivery and target acquisition.[24]

Continuing developments of microelectromechanical systems (MEMS) and potential developments in nanotechnology could provide an entirely new family of microminiature, intelligent weapons. Swarms of microminiature weapons could disable or destroy air or surface targets in support of the counterair mission. Intelligent materials systems, built at the atomic level by precisely placing each atom and molecule, could be powered by light for near limitless range and undetectable size. Inertial guidance systems, sensors and associated actuators, and their control by neural networked microprocessors could all be microsized through the application of MEMS and nanotechnology. Microminiature weapons could be aided by swarms of similarly sized intelligence, surveillance, and reconnaissance (ISR) systems. Swarms of microminiature weapons and sensor platforms could be launched by very small UAVs if the MEMS and nanotechnology development continues at its present rate.[25] The multipurpose UAV weapon system can perform a totally autonomous air-to-air or air-to-ground mission and, through advanced GPS guidance and preprogrammed mission parameters, can act in intelligent coordination with other UAVs or be remotely controlled from air, land, or sea bases by the ground pilot of 2025 (fig 3-1).[26]

The increasing threat to air vehicles will also be countered by the introduction of the FotoFighter into the inventory. The FotoFighter will use low observable technology coupled with conformal arrays of phased high-power solid-state diode lasers to provide simultaneous surveillance, tracking, designation, and thermal kill of targets, as well as communications.[27] The FotoFighter could form the backbone of the air strike capability, since it would be designed to be capable of high speed and maneuverability (hypersonic speeds and ±20 G capability) increasing its survivability; removal of the pilot would also increase opportunities for signature suppression.[28]

**Countermeasures and Countercountermeasures**

Wideband radars and multispectral detection systems will challenge the capability of the multipurpose UAV force to survive in hostile airspace. Active and passive stealth capabilities, low- and high-altitude operation,

**Source:** http://www.afit.af.mil/Schools/PA/gall3.htm, courtesy of Gene Lehman, AFIT/LSEC.

**Figure 3-1. Representation of UAV Ground Cockpit**

and low subsonic to hypersonic speeds will complicate detection by even the most advanced radars or other systems.

These capabilities provide survivability against surface and airborne threats. The camouflage, concealment, and deception of surface targets will complicate the surface attack portion of the offensive counterair mission. These factors will be offset by using wideband SAR systems, advanced IR detection from other UAVs and space assets, and the overall sensor synergism from surface, air, and space assets.

## Enabling Technologies

Target detection and identification will require advanced GPS and distributed satellites, along with artificial intelligence-based cooperation and distribution of mission responsibilities between platforms.[29] Cooperative and distributed electronically scanned arrays will support interaction between strike platforms and optimize targeting.[30]

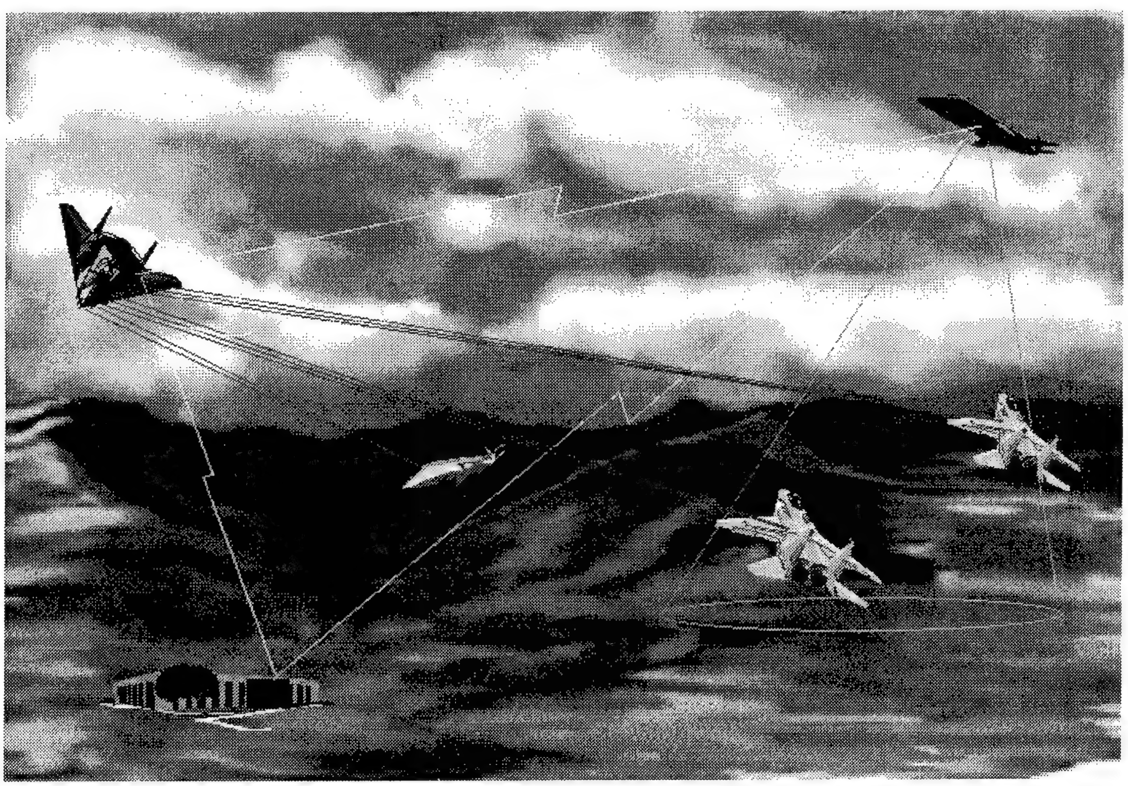
The key to successful implementation of UAV technology will be in active radio frequency and passive infrared (IR) stealth.[31] The aircraft itself must be constructed of high strength, lightweight, and reconfigurable materials.[32] To maintain on-orbit times and increase endurance, UAVs will use advanced fuels for lower specific fuel consumption and better all-altitude performance.[33] Hypersonic propulsion systems are needed to cope with the dense threat to air vehicles due to state-of-the-art air-to-air and surface-to-air missiles.[34] Part of the job will be to track friendlies, requiring advances in identification friend or foe (IFF) capability.[35] Detecting and tracking enemy aircraft means improvements are required in modular integrated avionics, including a downsized and wideband SAR.[36]

Finally, the high speeds and maneuverability of these systems will dictate advanced munitions and air-to-air missiles.[37] MEMS and nanotechnology could provide an exponential leap in microminiaturization for both weapons and platforms. To support the counterair mission in the high-speed, short-time-horizon battle space of 2025, mission planning and execution will require dynamic planning and execution control a la *New World Vistas*.[38]

## Concept of Operations

Multipurpose UAVs armed with sensors and/or weapons appropriate to the mission act in conjunction with surface, airborne, and space-based assets. The modular sensor and weapon bays discussed above provide mission planners the ability to mix and match components for optimal performance against the threat and targets. Potential threats and the mission to be accomplished determine the number and configuration of UAVs in a given mission package—threat detection, threat negation, active and passive decoys, sensor or communications relay, or armed for the defensive or offensive counterair mission. The FotoFighter would provide a unique quick strike capability against counterair targets of opportunity presented by short dwell targets such as missiles, missile launchers, or other hypersonic threat aircraft (fig. 3-2).

The UAV mission package is then launched from CONUS bases or airborne or sea-based platforms described above. This force package will use such air- and space-based assets as GPS and satellite communication links for autonomous



**Source:** Clipart elements from Federal ClipArt © 1995 with courtesy from One Mile Up, Inc., and Microsoft Clipart Gallery © 1995 with courtesy from Microsoft Corp.

**Figure 3-2. UCAV Strike Fighter (FotoFighter)**

operation over long distances and for terminal remote control if desired. Regardless of the mission, offensive or defensive counterair, armed UAVs will suppress enemy air defenses as necessary, destroy enemy aircraft and other systems in the air or on the surface, and return to CONUS bases or other platforms for refueling, rearming, and retasking.[39] At the same time, other UAVs operating independently or as part of the overall mission package identify and illuminate targets or threats for the strike UAVs, act as communications or data links, and provide real-time BDA.

The systems, technologies, and concept of operations described here provide the joint forces commander of 2025 with a multipurpose, long-range, lethal, and hard-to-detect and hard-to-kill autonomous weapon system or force package. Multipurpose UAVs accomplish the counterair mission of 2025 more efficiently and effectively, without risking the lives of pilots.

## Summary

As the US continues to attempt to do more with less, it becomes more and more likely the US will turn to UAVs to perform many of the missions requiring inhabited aircraft today. The counterair mission will be no exception. As described in this chapter, there is an opportunity to perform the entire counterair mission using UAVs. The current characteristics of UAVs—range, adaptability, and loiter time—when coupled with advances that will yield hypersonic strike capabilities, will allow the employment of UAVs in any environment against any type of adversary, from low-tech adversaries to peer competitors using stealthy cruise missiles or F-22 equivalents.

UAVs are even now coming of age, and decreased development, production, training, and replacement costs make them an attractive alternative to inhabited aircraft. In addition, the modular nature of much of our UAV fleet will allow tailoring of vehicles for specific missions, including air-to-ground counter-C2, SEAD, and conventional air-to-air against low-tech second wave air forces, as well as advanced fighter capabilities of peer adversaries. The FotoFighter, in particular, presents a significant leap in capability likely to be available in 2025. The addition of directed-energy weapons of variable lethality will be a considerable advance over the selectivity of current armaments for close-in and medium range-engagements. The flexibility and increased speed of hypersonic uninhabited strike aircraft will also allow these vehicles to avoid surface-to-air threats as simple as small arms and stinger missiles. This decreases the fragility of our counterair capability while enhancing survivability. Whether based in CONUS or on carriers, these assets can respond on demand, arriving on station in any AOR within hours, ready to conduct the mission without crew rest or prebriefing—the ground pilots having completed these activities while the UAV is en route to target. Once on station, trained ground pilots will assume control of the aircraft, allowing a level of fidelity near that achievable with pilots on-scene, increasing the flexibility of response.

The most difficult challenge will be to develop the technology required to support the strike UAV—the FotoFighter or its equivalent. In addition, to achieve the fidelity required to match a pilot on-scene, allowing the ground pilot to feel as if they are flying the mission will require significant advances. CONUS basing may also pose some challenges to situations that require a more immediate response; deployed UAV carriers would enhance responsiveness in crisis scenarios. Recovery and replenishment will require special attention, but some armament limitations may be overcome by the use of rechargeable DE weapons or nanoweapons. Even as the first of many UAV squadrons becomes operational, it is clear the enhanced capability and flexibility UAVs provide at lower overall risk and cost will drive the US towards an increased use of UAVs in the conducting the counterair mission.

## Notes

1. Lt Col Dana A. Longino, *Role of Unmanned Aerial Vehicles in Future Armed Conflict Scenarios* (Maxwell AFB, Ala.: Air University Press, December 1994), 9–12.

2. *New World Vistas: Air and Space Power for the 21st Century,* summary volume (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 60.

3. "New GPS 2R Satellites to Operate Autonomously," *Aviation Week & Space Technology,* 9 October 1995, 54; *New World Vistas,* summary volume, 25.

4. Martin L. van Creveld, *The Transformation of War* (New York: The Free Press, 1991), 208–9.

5. Bill Sweetman, "Major Milestones in US UAV Programme," *Interavia,* July/August 1995, 39–40; Bill Sweetman, "UAVs for Joint Forces," *Interavia,* September 1994, 62–64.

6. David A. Fulghum, "Air Force Prepares New UAV Acquisitions, Operations," *Aviation Week & Space Technology,* 27 November 1995, 52–54.

7. Defense Airborne Reconnaissance Office, *1995 Annual Report: Unmanned Aerial Vehicles (UAVs)* (Washington, D.C.: Office of the Under Secretary of Defense, Acquisition & Technology, August 1995), 6.

8. Ibid., 20–25; Bill Sweetman, "Major Milestones in US UAV Programme," *Interavia,* July/August 1995, 39–40; "UAV Force Concept," *Aviation Week & Space Technology,* 10 July 1995, 42–43.

9. David A. Fulghum, "International Market Eyes Endurance UAVs," *Aviation Week & Space Technology,* 10 July 1995, 40–43; Bill Sweetman, "Major Milestones," 39–40.

10. *New World Vistas,* summary volume, 41.

11. ***2025*** concept, no. 900441, "The Uninhabited United States Air Force," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

12. ***2025*** concept, no. 900777, "Smart Structure Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

13. *New World Vistas,* summary volume, 36.

14. *New World Vistas,* summary volume, 35; ***2025*** concept, no. 900135, "Offensive Unmanned Aerial Vehicle," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); "Unmanned Tactical Aircraft Concept," *Technology Initiative Game 95 (Systems Handbook),* 18–22 September 1995, 9–1, 9–2.

15. ***2025*** concept, no. 900172, "Miniature Precision Targeting UAV," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

16. Defense Airborne Reconnaissance Office, 40; David A. Fulghum, "International Market Eyes Endurance UAVs," *Aviation Week & Space Technology,* 10 July 1995, 40–43; ***2025*** concept, no. 900299, "Hunter-Killer Attack Platform," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 196); Bill Sweetman, "Major Milestones," 39–40.

17. *New World Vistas,* summary volume, 60.

18. ***2025*** concept, no. 900135, "Offensive Unmanned Aerial Vehicle," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 200006, "Unmanned Airborne Support Vehicle," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996) (Proprietary); ***2025*** concept, no. 900500, "Unmanned Fighter Bomber," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

19. ***2025*** concept, no. 900526, "Space-Based Airspace Control & Deconfliction System," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

20. "GPS Improves Military Weapons," *Aviation Week & Space Technology,* 9 October 1995, 56–57; ***2025*** concept, no. 900528, "Stealthy Lethal UAV," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900233, "The Very Small, Very Smart Bomb," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

21. *New World Vistas,* summary volume, 9; ***2025*** concept, no. 900233, "The Very Small, Very Smart Bomb," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

22. ***2025*** concept, no. 900638, "Autonomous Smart Bombs," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900244, "Global Positioning System Guided Munitions," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

23. ***2025*** concept, no. 900233, "The Very Small, Very Smart Bomb," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

24. *New World Vistas,* summary volume, 10.

25. Craig A. Rogers, "Intelligent Materials," *Scientific American,* September 1995, 154–57; Marvin Minsky, "Will Robots Inherit the Earth?" *Scientific American,* October 1994, 109–13; William B. Scott, "Micro-Machines Hold Promise for Aerospace," *Aviation Week & Space Technology,* 1 March 1993, 36–39; ***2025*** concept, no. 200023, "Surveillance Swarm," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900481, "Destructo Swarmbots," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

26. ***2025*** concept, no. 900278, "Real-Time Virtual Uplink with Unmanned Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

27. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the directed energy volume, 15 December 1995), iii.

28. *New World Vistas,* summary volume, 35.

29. Defense Airborne Reconnaissance Office, 40; *New World Vistas,* summary volume, 20, 43; "Cooperative Air-to-Air/Air-to-Ground Engagements-Distributive Fire Control," *Technology Initiative Game 95 (Systems Handbook),* 18–22 September 1995, 20–1.

30. "Cooperative ESA Jamming," *Technology Initiative Game 95,* 21–1.

31. *New World Vistas,* summary volume, 60.

32. Ibid., 52.

33. Defense Airborne Reconnaissance Office, 40.

34. *New World Vistas,* summary volume, 41.

35. David A. Fulghum, "Predator to Make Debut over War-Torn Bosnia," *Aviation Week & Space Technology,* 10 July 1995, 47–48.

36. Defense Airborne Reconnaissance Office, 40.

37. ***2025*** concept, no. 900233, "The Very Small, Very Smart Bomb," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

38. *New World Vistas,* summary volume, 58–59.

39. "C-17 Unmanned Aerial Vehicle (UAV) Airborne Platform," *Technology Initiative Game 95 (Systems Handbook),* 18-22 September 1995, 17–1, 17–2; ***2025*** concept, no. 900580, "In-Flight Air Refueling/Rearming of Strike UAVs," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

## Chapter 4

# The Virtual Trajectory: Air Superiority without an "Air" Force?

*New conditions require, for solution—and new weapons require, for maximum application—new and imaginative methods. Wars are never won in the past.*

—General of the Army Douglas MacArthur

As described earlier, the virtual trajectory assumes a globally minded US with plenty of technology and money to support military technological advancement. Its motto is Virtual Presence, Virtual Power. The premise: the US is a global power with an attitude, has a strong economy, and leverages an exponential growth in technology, but is reluctant to put its blood and treasure on the line routinely for questionable causes or outcomes. This, coupled with an increasing ability to locate, identify, and track both fixed and moving targets with high precision; a space-based force application ability (lasers, high power radio frequency [HPRF], high power microwave [HPM], etc.); and possession of surface-based weapons of a similar nature, leads to a reduction in the need for air superiority aircraft.

The America of 2025 is a global superpower in every respect, defined by a strong economy, political decisiveness, a resurgence in moral strength, worldwide recognition as an honest broker, and a position at the cutting edge of the technology of the day. However, there are some that wish to discredit or challenge the US's place in the worldview. The US's penchant for conflicts of minimal violence, with few casualties and little collateral damage, has placed renewed emphasis on precision in lethal application of force and a new stress on nonlethal force for subduing enemies. The result is a need for a space- and surface-based counterair capability for subduing any challenger using standoff weaponry.

The authors made some basic assumptions to frame our approach and demonstrate the need for a surface- and space-based counterair capability. The first assumption is that there would be a limited personnel and airframe base. Defense drawdowns would have reduced the availability of highly skilled pilots. As recently as the Gulf War, it was emphasized repeatedly that "no target is worth an airplane," and the American predisposition towards risking as few lives as possible is well known.[1] As such, inhabited airframes will be used only for key targets that cannot be hit from the surface or space without risking mission failure or collateral damage; the most likely use is in strategic attack or special operations roles. It was also observed during the Gulf War that the Iraqi population understood the US was targeting Iraqi military capability, and not the general population, because of the precision with which their military assets were targeted.[2]

The second assumption is the availability of adequate communications bandwidth to support the command, control, communication, computers and intelligence ($C^4I$) infrastructure required for coordinated real-time target acquisition, tracking, and battle management.

The third assumption is that the US will reap the benefits of huge leaps in technology that allow US armed forces to develop and deploy advanced space- and surface-based weapons. This assumption does not eliminate the possibility that a regional competitor, such as Iraq, could not

possess capabilities that would pose a threat to most of our forward deployed forces, or even continental United States (CONUS)-based assets.

A related issue is the impact of having an adversary as technologically capable as the US investing primarily in a virtual capability. In this case, the counterair mission as we know it would disappear, its requirements would likely be assumed by strategic attack and interdiction forces.

## Counterair Requirements

The requirements for this space- and surface-based counterair system can be broken down into three major areas: information collection and processing; situation awareness/command, control, and communications (SA/C$^3$); and force application systems. Target tracking and identification must allow identification of all friendly and threat aircraft in the area of responsibility (AOR) including airframe type, location, and heading, using both military, COTS systems, and commercial inputs. COTS processing capability will give the required computing power, and commercial multispectral and other inputs will provide additional data points to the threat identification process. When possible, the weapons load of enemy aircraft should be determined to allow the US to estimate the nature of the threat. Once an adversary is targeted, the weapon will require the capability to acquire a specific airframe to an accuracy that will allow submeter precision (particularly for lasers, to allow targeting specific control surfaces or weapons on the aircraft). This will be required since the most vulnerable parts of airframes are the pilot and the wing root.[3] Target acquisition and tracking systems will require a high degree of accuracy. Laser weaponry, in particular, will require accuracies to the centimeter for the more lethal effects. This is one area in which military research and development (R&D) will likely be required.

SA/C$^3$ systems are the linchpin of the effort. They will be required to ensure mission critical communications are being passed between target tracking systems, to the regional commander in chief's (CINC) battle management operations center (BMOC) and then to a target engagement node. Secure, jam-resistant communications must be available to support all phases of operations. The BMOC must be able to coordinate and direct all counterair assets and evaluate attack results. Battle damage assessment (BDA) can be accomplished by the same systems used for tracking and engagement in much the same way as the virtual presence capabilities described in *New World Vistas* where virtual presence allows for laser systems to provide attack, high-resolution imagery, high bandwidth point-to-point communications, optical IFF, and active remote sensing.[4] The biggest challenge will be sustainment of space-based systems. Once on orbit, space-based systems must either be maintained in-place (using a transatmospheric vehicle [TAV] or other technology) or replenished as required.

## System Descriptions

*Minimizing collateral damage is a requirement that will dominate all future contingencies and combat operations.*

—Col Richard Szafranski
*GEO, LEO and the Future*

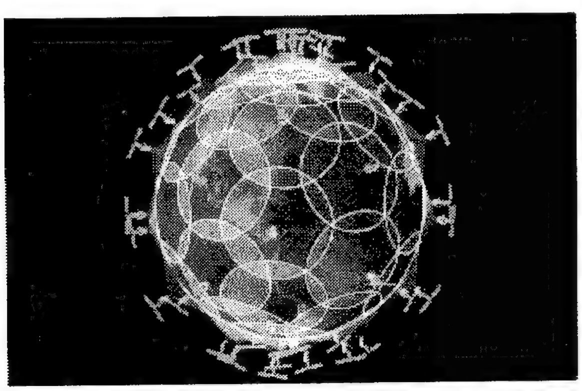
A virtual counterair capability will provide near-instantaneous precision strike with minimum collateral damage. To conduct the counterair mission, the virtual air forces rely on three key components: information collection and processing capability, SA/C$^3$ capability, and force application systems.

### Information Collection and Processing

The information collection system is based on the premise of performing wide area (global) surveillance at a low level of resolution, but looking for cues that require

detailed monitoring. These cues will trigger a switch to a reconnaissance mode providing multispectral, high-resolution information on activities in a given region or area of interest. A mix of phenomenologies will accomplish this. Using multiple phenomenologies is critical to seeing through enemy camouflage, concealment, and deception efforts to ensure we see what we think we are seeing. In 2025, distributed satellite constellations will be our eyes and ears, providing the global view described in *SPACECAST 2020.*[5] Distributed systems of small single-function satellites, working in planes much as GPS does today, will allow continuous coverage of the battle space in multiple frequency bands. A constellation of cooperative space-based radar satellites will be capable of providing a moving target indicator (MTI) capability and synthetic aperture radar (SAR) images similar to joint surveillance target attack radar system (JSTARS) (fig. 4-1). A complementary set of satellite receiver platforms can be used to perform geolocation of electronic emitters or bistatic imaging and tracking of noncooperative targets.[6]

Similar potential exists for electro-optical (EO) and infrared (IR) detection and tracking of targets. Multispectral EO and IR images can be merged with SAR images by superprocessors capable of correlating data from multiple sources and providing a high-resolution image of targets in near real time. Finally, a phased-array, space-based laser system will also be able to take high-resolution (submeter) imagery, further improving our capability. This will be accomplished by the use of a super-GPS time and position standard, allowing multiple laser images to be correlated with other sources of information to further refine target knowledge.



**Source:** http://leonardo.jpl.nasa.gov/msl/Quicklooks/Pictures/iridconst.gif, courtesy of Mike's Spacecraft Library.

**Figure 4-1. Distributed Satellite Constellation**

The space-based assets will be complemented by a series of fixed and mobile surface-based assets. Their capabilities will mirror those of their space-based counterparts; time-coded signals from individual satellites can be used for SAR image processing, MTI, and bistatic processing. A network of surface-based EO and IR sensors, as well as laser sites, will cover those targets obscured by high-level clouds, further adding to the information base on targets in any given AOR. Those areas covered by frequent low- to mid-level clouds will rely more heavily on the RF-based systems.

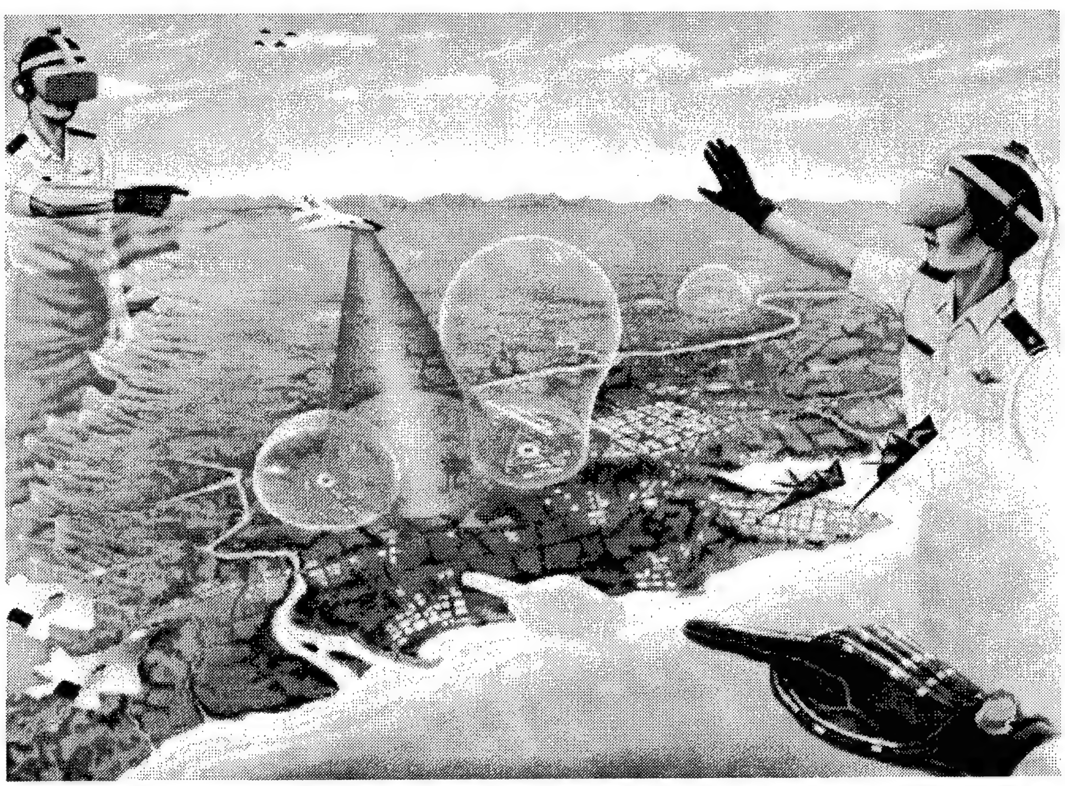
The focus of these collection systems is a multimode polyocular processing (M2P2) system that will correlate information using powerful, knowledge-based, image processing capabilities, providing detailed three-dimensional (3D) target images on demand. The combination of EO, IR, and RF phenomenologies, combined with processing designed to detect and identify enemy systems, will allow the US to see through almost any conceivable deception effort. The pseudoimage will be matched against IFF and threat data from space-based airborne warning and control system (AWACS) platforms and against standard target profiles, allowing determination of the weapons load as well as specific modifications made to the target that present special vulnerabilities we can exploit. Thus, a nominal resolution of 1-10 meters from any individual EO, laser, or IR sensor, combined with bistatic or other SAR images of up to one meter resolution, will result in submeter imagery to support target detection, identification, and tracking capabilities for force application worldwide. Communications

redundancy, using a combination of laser-crosslinks for space-to-space weapons platforms communications, and heavy reliance on redundant commercial communications encrypted for military use (particularly using wireless, cellular communications) will ensure worldwide connectivity for the entire system. The result is a system that lets US forces see in near real time what is happening in any region of the world at any time. The bottom line of our information collection and processing capability is our ability to continuously monitor the battle space.

### Situational Awareness/Command, Control, and Communications

The heart of any operation is its operations center. The air operations center of 2025 has evolved into part of the CINC's battle management operations center. The god's-eye view afforded the CINC and the JFACC, fed by the information collection and processing system previously described, gives the JFACC the ability to display the battle space in its entirety, or zoom down to a particular aircraft or engagement. This is accomplished using a holographic war room, much like the holodeck from "Star Trek," where 3D visualization of the battle space is possible from the synoptic (broad area overview) perspective, to allow monitoring and engagement throughout the AOR, down to a particular target, with the JFACC actively interacting with the holographic depiction, controlling engagement activity and monitoring the progress of the battle in near real time (fig. 4-2).[7]

The BMOC fulfills multiple functions. The war room allows not only real-time centralized control, but also, using very high-speed computers (up to 1,000,000 times faster than today's computers),



**Source:** http://www.afit.af.mil/Schools/PA/gall3.htm, courtesy of Gene Lehman, AFIT/LSEC

**Figure 4-2. Holographic War Room**

airspace deconfliction, battle simulations, expected outcomes in accelerated time modes, and BDA assessments. The speed-of-light nature of many of the laser and high-powered microwave weapons allows deconfliction of most engagements within minutes (or even seconds) of tasking.[8] Accelerated simulations allow the commander to evaluate courses of action in near real time. The computer will simulate the progress of an engagement based on the capabilities and doctrine of enemy forces using knowledge-based artificial intelligence software. As the BMOC learns more about how the enemy fights, this information will be applied to the engagement simulations, helping the JFACC select the best mix of weapons and weapon effects.[9]

The fast-forward outcomes can also be stored for comparison with the actual engagement, so the system can give the commander an empirical estimate of the outcome once a history of engagement activity is built. The results of both the simulations and the actual engagements will be stored as part of lessons learned for postconflict debrief and tactics modification. An assumed outcome to this will be a change from decentralized execution to distributed engagement. Distributed engagement is a result of the use of multiple small weapons to achieve a larger weapons effect, lack of time lapse between decision to engage and actual weapons on target, and a centralized command structure. A benefit of distributed engagements is a graceful degradation and increased survivability. A downside is the increased reliance on a single command center and its potentially vulnerable communications.

Part of the speed with which this activity is performed comes from the ability of the commander to use voice commands to establish ROE, pick targets, and finally specify weapons effects, from nonlethal to lethal. The commands can be as specific as "destroy the four F-16s crossing the Kuwaiti border" (centralized control—centralized execution) to "disable all enemy aircraft entering friendly airspace" (mission-type orders). The BMOC will recommend a series of options, which can be played out in the war room, allowing the commander to see the expected results, then select from one of the courses of action (COA) displayed. At that point, the commander will direct frag orders be sent to the individual weapon systems for execution. Based on inputs from the weapons sensors themselves, as well as our surveillance and reconnaissance systems, the actual battle can be displayed with insignificant time lag; the commander can observe the engagement as it is conducted, obtaining near-real-time feedback on the status of the mission. The closed-loop nature of engagement and feedback will allow rapid retargeting to ensure the CINC's and JFACC's objectives are met effectively and when required. The fog and uncertainty of war are significantly reduced, and adjustments to any engagement parameter (target, weapon, effect) can be made as required during the battle.

**Force Applications Systems**

High energy lasers (HEL) and high power microwave devices have been noted to be complementary.[10] Lasers are noted for their potential for destructive power; however, they require accurate targeting and a relatively benign environment (no clouds or overcast, smoke, or smog).

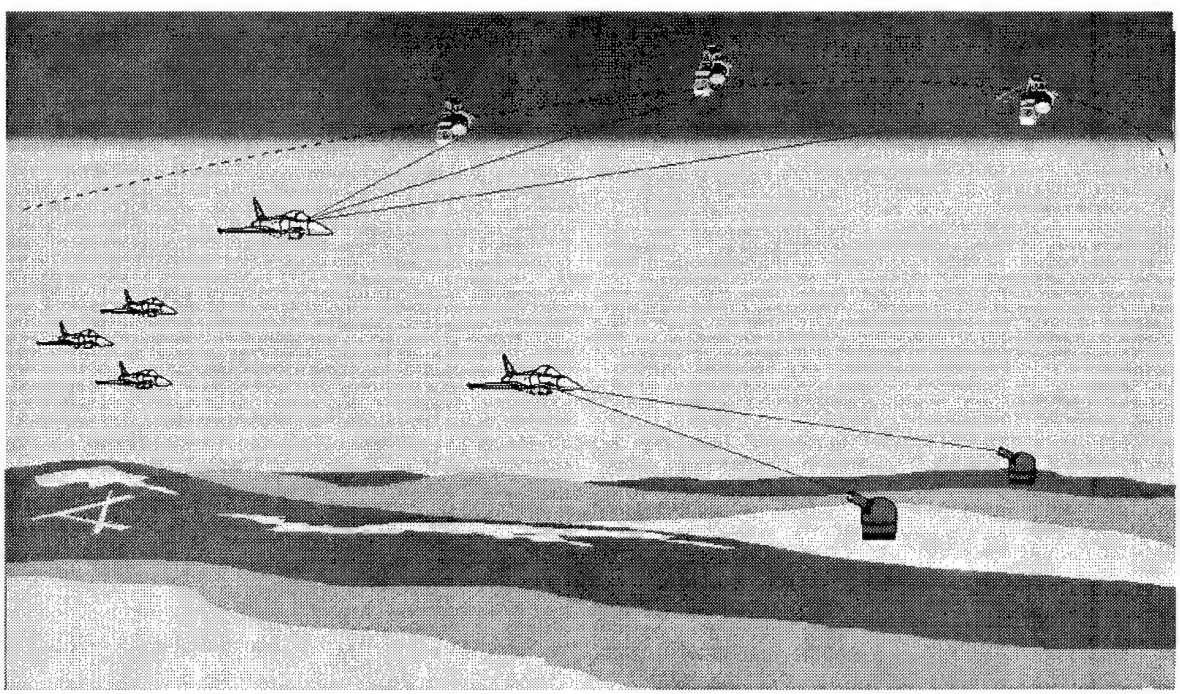
HPM weapons, on the other hand, are typically capable of less overt destructive power, but are capable of operating in virtually any environment and constitute an all-weather capability. They represent two sides of the same coin which can be leveraged in 2025.

**High Energy Lasers**

HEL weapons will constitute a part of both the space- and surface-based systems. Space-based lasers will come of age by 2025. A number of advances will make this possible. The first is a super-GPS capability that will provide a level of time accuracy to the nanosecond and position accurate to

the millimeter.[11] This capability will be tied into our constellation of distributed phased-array laser satellites (PAL-sats). These PAL-sats will not have to be the monster satellites envisioned in the Strategic Defense Initiative (SDI) era; they will be small, medium-power satellites, numerous, and easily replaced. By definition, space-based lasers are long-range weapons. Their power is derived from the ability to use a phased-array approach to putting energy on target. The phased array is managed by a central control satellite, using a low-power illuminator (also capable of imaging targets) to provide a phase reference for the deployed elements of the laser array (fig. 4-3). The phasing signal could also be used to communicate between elements of the system, passing targeting data, and so forth. Additionally, if the capability is developed, communication between phased-array laser elements could be accomplished using quantum communications methods, so phasing between elements could be communicated simultaneously.[12] Using the phase information in the phasing signal, each PAL-sat will use deformable mirrors made of microelectromechanical devices and phase-compensation measures such as phase conjugation to compensate for atmospheric and other effects. If coordination of these elements became too difficult or thermal heating of individual array PAL-sats became a problem, time-division-multiplexed lasing could be employed, with each PAL-sat firing in sequence against a particular point on the target, effectively providing a continuous laser from multiple-pulsed lasers.

The constellation approach simplifies each satellite, making it more affordable. The effect of the constellation is a graceful degradation of the weapon's capability if any one of the satellites is removed from operations due to weather, malfunction, or attack. It also allows for multiple weapons effects, which will be described below. Energy for such a system can come from



**Source:** Clipart elements from Federal ClipArt © 1995 with courtesy from One Mile Up, Inc., and Microsoft Clipart Gallery © 1995 with courtesy from Microsoft Corp.

**Figure 4-3. Friendly Phased-Array Lasers Targeting Enemy Aircraft**

multiple sources; the primary advantage in 2025 will be the development of composite materials that can change their characteristics on command. This is done using microelectromechanical systems (MEMS) deposited in the composite body of the satellite. When in one mode, the device can be rotated to minimize its signature, providing a measure of stealth. If the MEMS are rotated, like the highway billboards you see today, the devices soak up energy—either from the sun or a beam provided from the surface to recharge the weapon.

Surface-based systems are based on the same principles as the space-based systems. The phased-array approach allows surface-based assets to be used against the same target as the space-based system, and also allows targeting of medium-range targets. Hard kill of airframes becomes a greater possibility, permitting a larger range of weapons effects. It also helps defeat the mitigating effects of weather.

**Weapons Effects.** One of the greatest advantages of energy weapons is the variability with which they can be applied. Effects can range from nonlethal to lethal. Nonlethal effects can range from cloaking—using lasers to provide holographic camouflage in the visible portion of the electromagnetic (EM) spectrum—to hide assets from visual identification, to generating holo-threats that would appear to move in out of nowhere, confusing the adversary who must engage a virtual enemy or run for home.[13] To more fully deceive or confuse enemy onboard systems, HEL systems may require an adjunct whose only purpose is to provide a return for the enemy's radar—physical chaff launched by conventional means or rail gun, or RF deception of their radar systems. Granted, this assumes an unsophisticated enemy, but sometimes this may be enough psychologically. The combination of surface-and space-based systems is well suited for this type of deception.

A slightly higher level of lethality comes from a higher application of power. Effects such as canopy glazing, blinding, thermal effects (cooking off fuel or lubricants), or weakening structures is possible by varying the strength and width of the beam.[14] Lethal effects can be achieved by burning through control structures, fuel lines, or electronics, or causing foreign object damage (FOD) to the aircraft engine.

Finally, and probably one of the greatest reasons for fielding this capability, is the ability to target and destroy cruise missiles, intercontinental ballistic missiles (ICBM), and theater ballistic missiles (TBM). Whether the threat is against an ally overseas or to the continental US, a PAL-sat constellation provides a precision strike capability against even a multiple missile threat.

**Countermeasures and Countercountermeasures.** The downside to laser weaponry is its vulnerability to atmospheric effects. Although this vulnerability can be partially overcome by adaptive optics and wavelength adjustment, smog, fog, clouds, smoke, and dust can prevent successful operation. Local weather control may be possible to support operations in limited areas.

A prolific PAL-sat constellation and surface complement is also one way to defeat certain local conditions. Hardening against low-power laser radiation is also fairly simple; reflective surfaces go a long way in this direction, but the trade off is increased visibility. Laser-seeking devices could also be a threat to the weapons platforms themselves; in effect, when in operation, laser weapons designate themselves, a factor that needs to be considered. Defender satellites or space sentries in place to counter an antisatellite threat is a possible solution.[15] Visual or IR chaff are also options.

### RF and High Power Microwave/ Electromagnetic Pulse Devices

Space- and surface-based RF, HPM, and EMP devices will complement the laser capability of 2025 by providing an all-weather, day/night, variable lethality weapon. In addition to an all-weather capability, the greatest advantage of

HPM/EMP over laser is that it does not require the same level of precision for targeting; the target may try to evade, but the beamwidth of the HPM device will usually cover an area equal to or larger than the airframe, and, as long as tracking is to that order of magnitude, evasive tactics will prove useless. Collateral damage can still be minimized by proper beam formation and effects limited to the target(s). EMP is even less discriminating in its tracking and targeting requirements. However, it is a one-shot weapon, and the target has to be in the proximity of the device to be strongly affected, particularly for low-yield, high-explosive warheads.

HPM can be implemented in much the same way as lasers, using a phased-array approach, with both a distributed satellite constellation and surface-based elements. Beam shaping can be accomplished by using various combinations of the constellation and surface-based elements. HPM will be medium- (surface) to long-range (space) weapons. EMP will be implemented as a warhead weapon, being delivered either by rail gun or cruise missile, providing everything from close-in to long-range targeting, depending on the required speed of the response or extent of desired effects. Rail gun delivery from in-theater assets will be almost as timely as speed-of-light weapons and just as flexible. Surface-launched cruise missiles from CONUS or carriers provide a long-range, stand-off capability that can also serve as a deterrent.

RF weapons are a special case, because they represent a capability for a surgical strike. At any range, an RF weapon could be used to do anything from disrupt aircraft control to take over an aircraft (a.k.a. tractor beam).

**Weapons Effects.** HPM weapons are particularly effective due to the varied impact they can have on an adversary. As with lasers, HPM weapons can have nonlethal as well as lethal effects. The application of nonlethal HPM can result in thermal effects, such as weakening the structure of airframes, missiles, or command and control ($C^2$) facilities.[16] Continued application of microwaves against human targets (intentional or unintentional) can cause disorientation, discomfort, or long-term damage. At moderate power levels, the composite materials used in modern aircraft tend to absorb microwave radiation rather than reflect it, rapidly aging aircraft materials and destroying its stealth properties. Higher power levels of HPM can cause disruption of electrical circuits, particularly in sensitive integrated circuits or magnetic media. EMP can be used in a SEAD role by using shaped EMP charges to burn out receiver front ends in aircraft, $C^2$ facilities, or SAM sites. Another side effect of EMP bursts to targets on the surface and in the air is cable coupling, causing serious electrical system and structural damage.[17] RF weapons are capable of the simplest effect: basic ECM. This includes using space-based (or, where applicable, surface-based) systems to simply jam the front ends of enemy receivers, to generate false radar images to confuse the enemy's picture of the air war, or to insert false imagery into his data stream.

Lethal effects can vary from igniting fuel vapors and the consequent loss of the aircraft, to torching avionics and electronics with directed HPM or wide-area effect EMP bursts, causing loss of control. EMP bursts of sufficiently high power and/or proximity can cause aperture coupling, where the airframe itself couples the energy of the burst, thus causing destruction of all electrical components and damage to control surfaces, as well as possible destruction or damage to any human occupants.[18] In the RF realm, the most lethal effects will be the use of the tractor beam, where MEMS could be placed on an airframe, either by special operations forces, or by having them burrow into the avionics and electronics systems of an aircraft after it flew through a cloud of MEMS designed to penetrate the fuselage and implant themselves. Once implanted, a computer on our side could analyze the aircraft's control systems, and an operator on the surface could establish a link and take control of the enemy aircraft to force it

down, or merely land it at a friendly airfield for analysis and pilot debriefing.

**Countermeasures and Countercountermeasures.** The most significant countermeasure to HPM and EMP is stealth and structural design. If the aircraft is sufficiently stealthy, it will be difficult to track and apply the energy levels required to damage or destroy the aircraft. However, in 2025 few adversaries, if any, will have the capability to make their airframes invisible to all the forms of energy (EO, IR, microwave, laser, radar) used to detect, identify, and track their forces. Structural design can be used to mitigate the effects of aperture and cable coupling. A stealth paint can be applied to surfaces to further reduce visibility in selected portions of the EM spectrum.[19] Possible countermeasures are spectroscopic detection of the paint, exhaust tracking, or magnetic detection of aircraft.[20] These capabilities will make the ISR systems described under the Information Collection and Processing section above even more robust. The best counter-countermeasure (CCM) for US satellite-based capability would be the embedded MEMS in the composite structures described earlier that would allow the satellite to change its visibility based on the type of sensor attempting to track it, or a shell that deploys to protect the satellite, or the defender satellites mentioned above.

The RF/MEMS link is particularly hard to defend against. If a quantity of these MEMS is suspended in a slowly falling cloud above an air base, they would either fall onto enemy aircraft as they sit on the ramp, force adversary aircraft to fly through them to get airborne, or cause those aircraft to retreat to storage. In each case, the adversary's air capability is effectively grounded.

### Kinetic Energy Weapons/ Ground Launched Cruise Missiles

Kinetic energy weapons (KEW) and an improved ground-launched cruise missile (GLCM-X) capable of intercontinental ranges will provide an enhanced capability against hardened targets and targets of opportunity. The GLCM will replace the ICBM, mostly to enhance survivability. ICBMs are too easily tracked, and deviating from ballistic trajectories for ICBMs is tantamount to GLCM use in any case. Space-based KEWs are possible, but orbitology and time of flight will limit their application. Rapid progress in rail gun technology was seen during the 1980s, and kinetic energy weapons have been demonstrated using rail gun technology to propel warheads of up to 1000 kilograms (kg) and in excess of six kilometers per second (km/sec).[21] By 2025, advances in technology for these devices will yield vehicle-mounted weapons that could be located in the AOR and will give a response time that complements our energy weapons. Super-GPS combined with near-real-time target updates will allow medium- to long-range attacks on hardened airfields, aircraft revetments, airbase $C^2$ facilities, runways, or even aircraft in flight with both types of delivery systems.

**Weapons Effects.** The advantage of KEW and GLCM weapons is their capability against hardened targets and those targets requiring a tailored warhead. The ability to carry a sizable warhead allows the US to develop sophisticated nonlethal effects that can be delivered to submeter accuracy. Nonlethal effects include HPM/EMP warheads capable of producing effects similar to the space-and surface-based systems, less the phased-array aspect. However, proximity to the target and shaped warheads will compensate for this. The warheads can be delivered by either rail gun or GLCM, depending on the state of our forces in theater and the type of response the national command authority (NCA) desires—overt action in theater or covert delivery from CONUS. Other nonlethal warheads include FOD bombs (examples include webbing or netting over aircraft on the ground), suppression clouds, oxygen suckers, or highly tensile "silly string" to freeze control surfaces and keep aircraft grounded.[22]

Lethal effects can be achieved by MEMS that can damage or take an aircraft apart in

flight, drop submunitions on a runway, or deposit acid or other destructive liquids on airframe surfaces or airbase facilities.[23] An alternative antiaircraft artillery (AAA) method is to use rail gun warheads to eject a suspended net of high-tensile-strength steel that would shred aircraft control surfaces as the aircraft passes through it. This same method could be used for theater missile defense, disabling or destroying missiles and/or warheads in flight. The most direct approach is obviously to take a high explosive (HE) warhead right to the target—a GLCM warhead can take out a hardened facility, revetment, or C² facility. With a multiple reentry vehicle warhead and MEMS-controlled submunitions, it could take out an entire air wing on the ground. The rail gun would serve as a twenty-first century AAA, putting submunitions right through airframes at hypervelocities capable of ripping the airframe apart. In addition, the surface-based rail gun will provide another layer in the cruise and ballistic missile defense umbrella, complementing the capabilities provided by surface- and space-based lasers.

**Countermeasures and Countercountermeasures.** There are few countermeasures except extremely expensive hardening against HPM/EMP or stealth (antitracking) measures. The high speed of rail gun projectiles would negate evasion maneuvers.

A sufficiently small projectile, made of composites and moving at hypervelocity, would be hard to detect, much less counter. The GLCM-X would be designed to go against hard, fixed targets or produce wide-area effects requiring large payloads/warheads; given this, the only effective counter is successful camouflage.

## Enabling Technologies

The enabling technologies allowing the successful implementation of the counterair mission using space- and surface-based assets can be grouped into the same categories as the areas requiring development: information collection and processing, situational awareness/C³, and force application. The key technologies supporting information collection and processing include advanced space-based radars capable of SAR, MTI, and bistatic detection; high-speed computing and real-time linking to support space- and surface-based phased-array laser and HPM capability; timely, cost-effective launch of tailored, distributed satellite constellations; and distributed processing of multimodal information for real-time tracking of targets.

The requirements for SA/C³ technologies include allowing real-time displays of order of battle, enemy and friendly COA generation, and wargaming of outcomes. This includes artificial intelligence/knowledge processing systems capable of correlating multispectral, multimodal information. Fused, correlated information would be used to generate enemy and friendly COAs and three-dimensional holographic presentation and real-time simulation of enemy and own force activities in fast forward modes. Combined with the distributed processing of target information, this could also provide near-real-time BDA.

Weapons application technologies are centered around advanced GPS, capable of nanosecond accuracy and millimeter precision, and high-resolution optics, beam directors, and deformable mirrors for laser applications. The phased-array lasers and HPM also require the development of phased-array timing/phase synchronization signals (such as time-coded reference signals or quantum nodal communications) to allow timely communications between physically separated array elements. Composite materials, with imbedded MEMS capable of changing states to accommodate stealth (energy absorption), power accumulation (energy conversion), or active transmission are needed to support the stealth aspects of our platforms. High power RF and HPM technologies must be developed to make spaceborne platforms viable. Mobile, moderate payload (up to 1000 kg), hypervelocity rail gun delivery systems are needed

to support the rapid response of surface-based EMP and HPM weaponry.

## Concept of Operations

The BMOC is the heart of counterair operations. Using all-source information generated by space- and surface-based sensors, the holographic war room will give the CINC and JFACC the ability to monitor friendly and enemy forces in near real time. The JFACC, using voice commands, will be able to ask the war room to "show enemy air forces," followed by "show enemy IADS." After reviewing the enemy order of battle, he can ask the system to "show probable enemy actions and targets." Once requested, the system will examine the enemy ordnance load and fuel capacity (gathered by space- and surface-based SAR, EO, and laser imagery), and project their tracks to and from targets. The JFACC will then ask the system to "show own forces," and all offensive and defensive systems and their effectiveness envelopes will come up. At that point, the commander's intent will have to be specified in terms of the mission: deter, disrupt, or destroy enemy assets. Depending on the enemy, the target, and the CINC's objectives, the JFACC will request COAs appropriate to the mission. After reviewing the COAs in fastforward mode, one will be selected and targets identified and designated in the war room. One fallout of the responsiveness of energy weapons to tasking is the requirement for centralized control and centralized execution of these systems. The immediacy of the impact of weapons use and requirements for real-time deconfliction with other air and surface forces requires control from the war room. This need is reflected in the way space and surface counterair forces are tasked. The degree of damage or destruction of each target will be specified before engagement, and target parameters passed directly to the weapon systems.

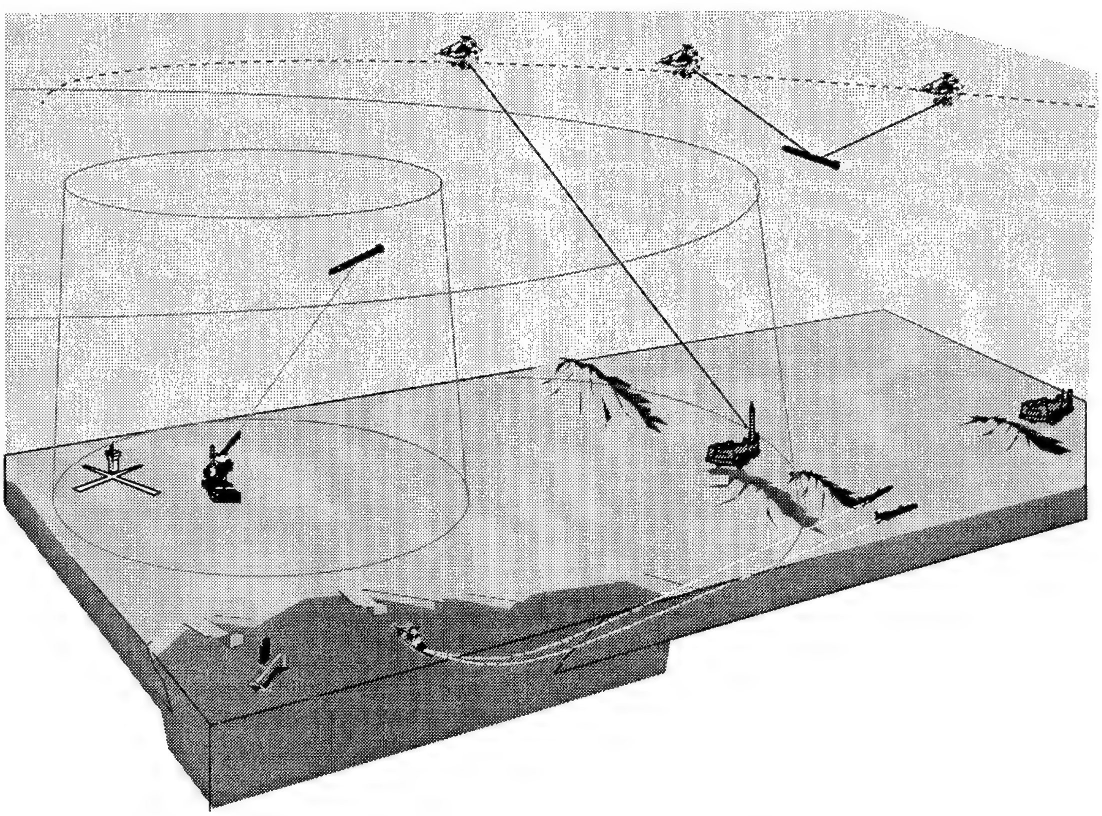
Most adversaries will be deterred by the recognition that, as a global superpower with worldwide virtual presence, the US is capable of quickly identifying enemy actions and responding before they pose a threat. Because of this, most operations will likely be deterrent missions, demonstrating capability and resolve to the enemy. Simple methods such as holographic projection of an air threat against the adversary would be attempted first to scare him off. As the adversary increases the aggressiveness of his posture, the US could respond in kind by increasing the threat to enemy air forces, using the MEMS cloud or GLCM to keep enemy aircraft grounded. If deterrence fails altogether, a destruction COA will become more likely. The weapon of choice could be selective lasing of vulnerable airframe surfaces, disabling HPM bursts, or airspace control devices such as the silly string or steel nets. Active high-power lasing, RF, or HPM bursts will disable, destroy, or ground large segments of the enemy air capability. Near-real-time BDA will allow for rapid retargeting of assets; one of the advantages of space-based weapons is that they are always forward deployed. In this instance, if high-energy lasing of a penetrating aircraft were required, real-time reporting from the laser platforms would be combined with EO, IR, and SAR imagery to determine if the target was "heating up," had exploded, or gone down in near real time. The tractor beam capability will be reserved for high-value air assets and reconnaissance vehicles. This will allow the US to determine the type of enemy systems and capabilities, and to build countermeasures or deception programs around these systems. This will also increase US stature in the world community by reducing the death and destruction of airframes and pilots, and give the US another source of human intelligence (HUMINT) from pilot debriefings.

Cruise missile and ballistic missile defense (BMD) will be a primary function of space- and surface-based counterair forces. Part of the driver for the global surveillance and focused reconnaissance capabilities of the BMOC will be to accommodate the requirement for constant vigilance of the

cruise and ballistic missile threat. The combination of laser, HPM, and rail gun payloads will provide a multitiered, all-weather defense against ballistic missiles (fig. 4-4). The M2P2 processing capability described above will allow the determination of location, velocity, and probable launch and impact points. The war room will provide detail on the nature of and confidence level of the threat, but the crews on watch in the BMOC will be the human in the loop to ensure the threat is identified quickly—within 60 seconds—but verified before destruction. Although 60 seconds is not a significant improvement over detection and warning times today, the problems of detecting stealth missiles will complicate the problem, and the ability to begin neutralizing the threat within seconds of identification provides significant leverage that does not currently exist.

## Summary

The key to the success of the systems described above is matching the capability to possible threats. This paper described the range of threats. The applicability of directed energy weapons, cruise missiles, and nonlethal munitions payloads varies across the spectrum. The strength of the systems described above is in their versatility and responsiveness. Directed energy weapons have their strength in their ability to engage at everything from very low to very high power levels, increasing from nonlethal disruptive effects to lethal destruction at the flick of a switch. Cruise missiles will



**Source:** Clipart elements from Federal ClipArt © 1995 with courtesy from One Mile Up, Inc., and Microsoft Clipart Gallery © 1995 with courtesy from Microsoft Corp.

**Figure 4-4. Multitiered (Laser, GLCM, Rail Gun) Missile Defense Capability**

be highly accurate, delivering any payload at high precision at any given time for measured effect. Rail guns give the added versatility of being able to put "steel (or plastic) on target" in a short period of time, also with the possibility of multiple payloads.

The weakness of DEW is the flipside of its strength—once engaged, the mission can be halted, but whatever damage is done, is done. Cruise missiles can be destructively aborted; rail gun payloads lie somewhere between the two, depending on distance to target and the nature of the payload. None of these systems carry much finesse once a mission has started; a human in the loop is not the same as a human on the scene, and the fidelity of feedback is much more limited.

Even a fused picture of the battle space will not yield the same insights as a pilot in the cockpit engaged in a flyby of possible hostiles. For this reason, UAVs or inhabited aircraft are much better suited to low tech or second wave adversaries engaged in such cat-and-mouse tactics as airspace infringement or insurgency. The significant advantage of these systems is, as previously described, their ability to instantly engage a target. Distributed space-based systems, in particular, provide a method of reaching targets worldwide on a moment's notice. This is crucial when considering the theater ballistic missile, ICBM, and cruise missile threat of 2025.

The surface- and space-based systems described in this trajectory also enjoy the advantages of low fragility; they appear less vulnerable as a system because of their distributed nature. The distributed engagement concept also allows for a multiple simultaneous target scenario over a large (basically global) engagement area— a direct result of the forward deployed aspect of space assets. This in turn supports the ability to train as you fight, which is inherent in these systems since, to the operator, any simulation seen during training will appear identical to what would be seen in an actual engagement.

The most daunting aspects of fielding these systems are the technological and financial requirements. The technological improvements required to implement a space-based phased-array laser or HPM capability are an order of magnitude or more increase from state of the art in 1996. The associated cost for research and development and deployment are significant for all the elements of the system—information collection and processing, SA/$C^3$, and force application systems.

In the final analysis, the ability to imme-diately reach out and touch a target with both lethal and nonlethal consequences will provide a significant deterrent as a key component of US overall counterair capability.

**Notes**

1. Thomas A. Keaney and Eliot A. Cohen, *The Gulf War Air Power Survey Summary Report* (Washington, D.C.: Government Printing Office, 1993), 248–49; and Richard H. Shultz, Jr., and Robert L. Pfaltzgraff, Jr., eds., *The Future of Air Power in the Aftermath of the Gulf War* (Maxwell AFB, Ala.: Air University Press, July 1992), 303.

2. Richard P. Hallion, *Storm over Iraq: Air Power and the Gulf War* (Washington, D.C.: Smithsonian Institution Press, 1992), 199.

3. "New World Vistas: Air and Space Power for the 21st Century" (USAF Scientific Advisory Board, unpublished draft, the directed energy volume, 15 December 1995), 56.

4. Ibid., x.

5. *SPACECAST 2020 Executive Summary* (Maxwell AFB, Ala.: Air University Press, 1993), 12.

6. *New World Vistas: Air and Space Power for the 21st Century, summary volume* (Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995), 20.

7. ***2025*** concept, no. 900385, "3-D Holographic Battlefield Display," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900161, "Holographic C2 Sandbox," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900417, "Battlespace Awareness Holosphere," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

8. ***2025*** concept, no. 900526, "Space-Based Airspace Control & Deconfliction System," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

9. ***2025*** concept, no. 900414, "Artificial Intelligence: A New Aircrew Member in Tomorrow's Combat," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900522, "Space-Based AI-Driven Intelligence Master Mind

System," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

10. "New World Vistas" (unpublished draft, the directed energy volume), iii.

11. *SPACECAST 2020*, 13.

12. ***2025*** concept, no. 200013, "Quantum Effect Communications," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996). (Proprietary)

13. ***2025*** concept, no. 200015, "Distortion Field Projector," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996) (Proprietary), ***2025*** concept, No. 900313, "Spaceborne/Airborne Hologram," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** concept, no. 900336, "Cloaking," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

14. Lt Comdr James Todd Knight, "Aircraft Survivability: Vulnerability to Directed High Energy Weapons" (Thesis submitted to the Naval Postgraduate School) (Monterey, Calif.: Naval Postgraduate School, December 1986), 126.

15. ***2025*** concept, no. 900371, "Automated Space Sentries," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

16. Knight, 51, 110.

17. Ibid., 45, 47.

18. Ibid., 45, 46.

19. ***2025*** concept, no. 900605, "Active Cloaking Film/'Paint'," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

20. ***2025*** concept, no. 900647, "Jet Exhaust Tracking AAMS/SAMS," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996) (Proprietary), ***2025*** concept, no. 900508, "Magnetic Detection of Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

21. *Study of Oblique Detonation Wave Scramaccelerator for Kinetic Energy Weapons and Lethality Testing* (Advanced Projects Research Inc., February 1990), abstract.

22. ***2025*** concept, no. 900258, "Oxygen Sucker," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

23. ***2025*** concept, no. 900436, "Runway Targeting Smart Munition," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); Wing Commander E. E. Casagrande, *Non-Lethal Weapons: Implications for the RAAF* (Royal Australian Air Force Air Power Studies Center, November 1995), 15–16.

# Chapter 5

# Synthesis

*The bedrock of what we do is air superiority . . . we want to dominate the other guy's airspace.*

—Gen Ronald R. Fogleman

The world of 2025 is a world of varied threats. The air threat can be as simple as a terrorist with stinger missiles or Cessnas flying from Latin America or Cuba. On the other end of the scale, the threat could be long-range cruise missiles from Iran, a Chinese stealth capability much the same as the F-117, a Russian air-based laser, or a North Korean ballistic missile.

From the previous discussion several conditions can be derived that must be met for the successful execution of the counterair mission. The first condition is that the US must be able to counter the full range of threats, from the surface to the edge of space. These threats encompass the full range from small arms to lasers. What is common to the airborne threats is that they cease to become threats once they are no longer airborne.

This leads to the second condition, one based on the definition of counterair operations—that mission success is based on the neutralization of the enemy's air forces. This can be accomplished by keeping them on the surface or, if airborne, to remove them from the protected/defended airspace and hence remove the threat they pose.

The third condition that must be met for successful execution of the counterair mission is to establish the freedom to operate in any airspace with impunity—the crux of air superiority. The threat the US must deal with is the antiair capability of today and tomorrow—something as simple as a shoulder-launched antiaircraft missile to a space- or surface-based laser similar in capability to the type described in our virtual trajectory.

Over time, we have recognized a fourth condition—there will be an increasing need to perform the counterair mission in both a lethal and nonlethal manner. A priority is reducing the exposure of air assets and their operators to enemy fire.

The fifth condition is derived from the increasing ability to project great power over great distances in a short period of time. This mission must be performed both at short range and at increasingly long ranges—and not only protect US airspace at home, but also be able to project power from CONUS to halfway around the world at a moment's notice.

## Analysis

A critical assumption is derived from the previous analysis and the conditions described above: the need for a mix of inhabited and uninhabited aircraft as well as surface- and space-based systems. The need for inhabited aircraft is driven by the convergence of two forces—the nature of a second wave airpower threat and the fact that in our democracy we will always consider leaders, at all levels, responsible for their actions. The inescapable conclusion is that some threats require not just a human in the loop, but a human on the scene. At no point in the previous discussion has the assertion been made that any of these systems is foolproof; in a given situation, one may present a better solution than another. The dominant battle space awareness provided by the ISR and situational awareness systems of 2025 will never provide perfect knowledge of enemy capabilities or intentions.[1]

Examples are the probing missions conducted by the USSR near US airspace in Alaska during the cold war and the shootdown of private aircraft near Cuba in February of 1996. In the future, US airpower will encounter aircraft in international airspace with questionable or unknown intentions. Even with the near-real-time relay of information, these circumstances will spawn situations where nothing can replace the intuition, or gut instinct, of a pilot flying combat air patrol (CAP), making the determination based on information from offboard, onboard, and experience.

The positive control implied by a pilot on-scene is a powerful deterrent as well; an adversary may be much less likely to attempt to down an inhabited aircraft in a nonprovocative situation for fear of an adverse US or international response. It is also likely that as countermeasures improve, there may be situations where inhabited as well as uninhabited vehicles will be cut off, losing their eyes and ears. The advantage of inhabited aircraft is that the pilot will be much more capable of recovering from the situation, and possibly taking advantage of it, whereas if the UAV is cut off, it will require a fail safe that will, at best, allow it to return to base.

On the other hand, in the case of a general war scenario, uninhabited vehicles, commanded from a remote operations center for preprogrammed missions or via a real-time data link may be the weapon of choice. In this case, the FotoFighter described in *New World Vistas* may be the right vehicle for taking out enemy targets; combined with uninhabited reconnaissance, command and control, and relay aircraft, the FotoFighter may be the best all-around choice for close-in and medium-range targets.

The disadvantages of the inhabited aircraft have been enumerated many times: high training costs, limited number of platforms, limited number of pilots, and limited number of target engagements per platform. An increasingly hostile threat environment, including hypervelocity missiles with multimode seeker heads, makes conventional aircraft increasingly unattractive in terms of the cost of a single failed engagement. This must be balanced with the projected relative ease and timeliness of the application of high-energy weapons, whose maintenance costs may be high and where depth of magazine, particularly in the space-based situation, may be limited.

The downside of aircraft is reaction time. The best equipped strike fighter is useless if it shows up after the battle is lost—and reaction time will be at a premium against our more sophisticated foes in 2025. Adversaries will increasingly have access to weapons that today seem exotic, such as stealthy cruise missiles.[2] This is where US space- and surface-based capabilities come to the fore. The ability to detect, acquire, identify, then destroy the enemy's counterair capability within seconds will be the driver behind this capability. It will also provide a more robust deterrent capability, since mobile surface- and particularly space-based assets are always forward deployed, basing is not a problem, and there are no assets to move to a forward area under the global grid interconnectivity envisioned for 2025.

The forward deployment of space-based weaponry and the ability to instantly apply firepower is particularly important against the cruise and ballistic missile threat. Once the threat is identified, time is crucial. Delays in detection and identification due to active and passive stealth measures will mean the leverage found in the immediacy of figuratively putting steel on target make DE weapons a key element of our counterair capability. The complementary nature of high energy lasers, HPM, and rail gun kinetic energy weaponry will provide an all-weather, multitiered defense against the ballistic and cruise missile threat of 2025.

The result of the analysis is the identification of a need for a combination of capabilities, a synthesis of the three trajectories. The identification of the strengths and weaknesses

demonstrates how the capabilities described in each trajectory complement each other. The combination yields a counterair triad that matches capabilities against threats, and best succeeds at meeting the conditions for successful mission execution described above.

## Comparison

Four approaches were developed for conducting the counterair mission based on the evolutionary, penurial robophile, and virtual trajectories, plus a fourth approach defined by the system of systems combination of all three: the counterair triad. Table 1 compares each of the four approaches and maps it against a set of criteria describing the capabilities required in 2025. A four-level gray scale was developed for comparison of each approach against those criteria. On this scale, white means the criteria were not well covered or the capability is limited, with gradations up to black, meaning the criteria is well covered or the capability is robust. These criteria allow a side-by-side comparison of all four approaches to better visualize what each brings to bear in the conduct of the counterair mission.

1. *Applicability to Multiple Scenarios.* There are three types of scenarios at a high level—a regional competitor (a medium-tech, second wave adversary such as Iraq or North Korea); a peer competitor (the old USSR or a future China); and a niche competitor (terrorist/insurgency, etc.). Measure of merit: white = covers none; light gray = one of the three; dark gray = covers two of the three; black = covers all.

2. *Capability Leap.* Measures whether the capability is an evolutionary change or tends to revolutionary improvement in capability. Measure of merit: white = current capability; light gray = minor improvement in capability; dark gray = significant improvement in capability; black = order of magnitude improvement (revolutionary).

3. *Range.* Applicability to close-in (less than 150 miles), medium-range (150–1,000 miles), and long-range (1,000+ miles) engagements. Measure of merit: white = none; light gray = engages at one range set; dark gray = engages at two range sets; black = at all ranges.

4. *Selectivity.* Describes the range of options provided by the approach, from lethal to nonlethal. Measure of merit: white = no capability; light gray = nonlethal; dark gray = lethal; black = selective lethality (nonlethal to lethal).

5. *Response Time.* Indicates the time between the decision to employ force until action against the threat. Measure of merit: white = days; light gray = hours; dark gray = minutes; black = seconds.

6. *Flexibility.* Reflects the ability to provide a flexible response in the mission profile prior to weapons employment. Measure of merit: white = none; light gray = some; dark gray = routine; black = selective.

7. *Fragility.* Indicates the perceived cost of the loss a of single asset—aircraft, spacecraft, cruise missile, and so forth. and/or loss of life. Measure of merit: white = very high; light gray = high; dark gray = medium; black = low.

8. *Targeting.* Describes the number of potential target engagements per sortie. Measure of merit: white = single; light gray = few; dark gray = many; black = lots.

9. *Weapons Engagement Area.* Indicates the effective area the system can engage in at one time. Measure of merit: white = visual range; light gray = sensor range; dark gray = regional (beyond platform sensor range); black = global.

10. *Basing Limitations.* Describes the type of basing required for each approach. Measure of merit: white = in the area of operations; light gray = in the CINC's AOR; dark gray = CONUS; black = flexible.

11. *Cost.* Reflects the relative cost of deployment/employment of the approach in each approach. Measure of merit: white = very high; light gray = high; dark gray = moderately high; black = baseline.

From this comparison it is clear that each approach has certain strengths and weaknesses. The evolutionary approach is

**Table 1**
**Comparison of Counterair Approaches**

| Criteria / Approach | Evolutionary | Penurious Robophile | Virtual | Triad |
|---|---|---|---|---|
| Applicability | | | | |
| Capability Leap | | | | |
| Range | | | | |
| Selectivity | | | | |
| Response Time | | | | |
| Flexibility | | | | |
| Fragility | | | | |
| Targeting | | | | |
| Weapons Engagement Area | | | | |
| Basing | | | | |
| Cost | | | | |

more achievable given today's state of the art and can accommodate more sensitive situations through direct contact of the pilot on-scene, but is more fragile and less responsive than the other two to immediate threats. The penurious robophile approach has more overall strength, but lacks some fidelity, even with ground pilots and, like the evolutionary trajectory, suffers from an inability to respond to immediate threats. The virtual trajectory is best suited for situations requiring an immediate response (overseas threats or cruise missiles), but requires the greatest leaps in technology, most significant cost, and the most trust in the system—not necessarily a given when such significant responsibility and accountability is demanded of our people. The fourth approach—the triad—covers the approaching threat and required capabilities of 2025 best. A balance of response time, lethality, fidelity, and cost, the counterair triad allows us to respond with the right amount of force at the right time in the right place.

The analysis of the three trajectories allows us to put in perspective a more comprehensive approach to the accomplishment of the counterair mission. Each trajectory had its own approach to the counterair problem based on a particular set of assumptions. The convergence of these trajectories leads to a solution set all its own—where the triclinic of these trajectories meets to address a wide range of threats in a variety of environments. The result of this synthesis are found in the next chapter.

### Notes

1. Col Jeffery R. Barnett, *Future War: An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala.: Air University Press, January 1996), 83.

2. Ibid., 111.

# Chapter 6

# Recommendation

*You should not have a favorite weapon. To become over-familiar with one weapon is as much a fault as not knowing it sufficiently well. You should not copy others, but use weapons which you can handle properly. It is bad for commanders and troopers to have likes and dislikes. These are the things you must learn thoroughly.*

—Miyamoto Musashi

The overall requirements for the counterair mission are based on the conditions for successful mission execution described in the previous chapter. The trajectories presented reflect the need to examine the extreme ends of the scale on which counterair missions may be conducted, using an "anything but" criteria. The first trajectory examined "what if technology does not advance much, or the money is not there to implement many changes." The second trajectory looked at how counterair would be conducted if we used anything but inhabited vehicles. The final trajectory examined how the counterair mission would be conducted using anything but aircraft. Having reviewed these potential outcomes, we realize that in 2025 the counterair mission would and must actually use a mixture of systems from each of the three. There are some common themes running through all of the trajectories, and these will be a part of the counterair mission in 2025—the need for enhanced, real-time intelligence, surveillance, and reconnaissance (ISR), using multiple modes of detection—RF, IR, EO, SAR, spectrographic analysis, laser imaging, magnetic anomaly detection, passive and active intelligence collection, and so forth. Each trajectory also clearly recognized the human propensity for visualization, and identified the need for an operations center based on a near-real-time, three-dimensional presentation of the battle space—a holographic war room. The war room will use advanced knowledge processing to synthesize a visual view of the threat based on multimode polyocular processing, using the inputs from the many multispectral eyes available to generate a detailed image and depiction of threat capability for course-of-action generation, simulation, selection, and mission execution. The glue that holds these elements together is communications—a robust mix of dedicated military and civilian communications. The combination of information processing to allow situation awareness at a level of detail that can be tailored to the user or operation, combined with real-time simulation and observation of the friendly and enemy actions, and connected by a global grid of intermeshed communications nodes, allows prompt and sustained action in support of air operations.

The varied threat will require a mix of response capabilities—from low-threat, low-speed, nonlethal responses to high-threat, high-speed, lethal response. In each of the three trajectories, there are cases where the capability described is wholly appropriate for the situation. The high-probability second wave threat makes conventional aircraft attractive; the need for stealthy, low-cost, less personnel-intensive, AOR-specific reach and force application make uninhabited vehicles an approach whose time has come; and the need to counter high-speed, high-lethality threats such as TBMs, ICBMs,

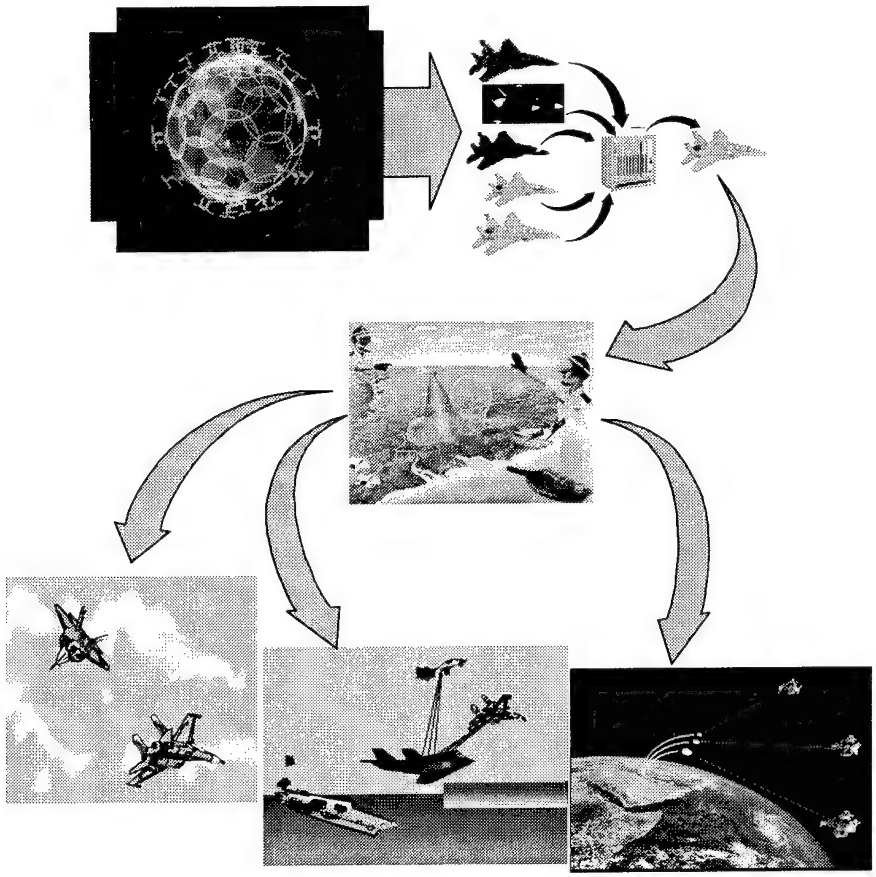
or cruise missiles, or the need to react on a moment's notice with power projection to a deployed force or ally halfway around the world makes surface- and space-based weapons an excellent choice. This drives the need for inhabited and uninhabited aircraft, as well as surface- and space-based capabilities for the world of 2025.

## Concept of Operations for 2025

The counterair forces of 2025 will use the information collection, processing, distribution, and presentation methods described in each of the three trajectories. Distributed satellites, using hyperspectral collection methods, will be processed in real time to provide everything from wide area, synoptic views down to details on specific targets. The commander in chief or the joint force aerospace component commander (JFACC) of 2025 will be able to use a holographic war room to visualize the battle space, ask the battle management operations center processor to show suspected enemy courses of action, suggest friendly courses of action, and project outcomes. The friendly courses of action will be based on the nature of the threat and the CINC's intent. Simulations can be run for various combinations of friendly versus enemy COAs, and using elements of chaos theory, projections made on the utility and chance of success of the responses. From these, the CINC or JFACC can make the appropriate choice and implement it in near real time.

The key to determining which assets are required to perform the counterair mission of 2025 is a function of the threat, the required level of deterrence, disruption, or destruction of enemy air forces, and the timeliness of the required response. Minimal threats require minimal, nonlethal response, but politically sensitive operations may require feedback that is only possible with inhabited aircraft. More substantive threats, such as F-22 type aircraft or uninhabited strike aircraft such as an enemy FotoFighter, may require lethal to nonlethal responses that can range from short to long range, and varied amount of time to react, making either inhabited, UAV, or surface- or space-based response appropriate. Antiair rail guns, with projectiles moving at hypersonic speeds, will provide a lethal air defense capability against enemy UAVs. At the extreme end of the spectrum, the threat may consist of hypersonic stealthy cruise missiles, theater ballistic missiles, or ICBMs where a long-range, immediate response is required, making surface- and/or space-based assets the only appropriate response (fig. 6-1). The end result is a triad approach based on threat, intended effect, and immediacy of response. The options available to the JFACC will be composed of the systems described by our three trajectories. The JFACC will apply the portion of airpower that best suits the mission objective, threat, and desired weapons effect, and his instructions will be passed via his holographic war room. The JFACC will watch his instructions being carried out and get BDA in near real time. The common link that will drive this capability will be communications capability. The importance of this capability cannot be overemphasized as we look forward to 2025.

The result is a concept of operations based on systems from all three trajectories. As a singular superpower in a multipolar world, the complexities of the counterair threat posed to the US will only increase. The capabilities-based response made possible by the counterair triad described above ensures the US air superiority against each of the threat environments posed above, whereas any one alone will not. The overlapping synergy of the counterair system of systems—the counterair triad—will ensure air superiority for the US in 2025 and beyond.



**Source:** Clipart elements from Federal ClipArt © 1995 with courtesy from One Mile Up, Inc., and Microsoft Clipart Gallery © 1995 with courtesy from Microsoft Corp.

**Figure 6-1. Counterair Triad Concept of Operations**

## Conclusion

*When offensive weapons make a sudden advance in efficiency, the reaction of the side which has none is to disperse, to thin out, to fall back on medieval guerrilla tactics which would appear childish if they did not rapidly prove to have excellent results.*

—Gen G. J. M. Chassin

*In war the chief incalculable is the human will.*

—B. H. Liddell Hart

The three trajectories presented in this paper are the culmination of a comprehensive analysis of what the counterair mission might entail in the year 2025. Each was developed with an eye toward continuing and sometimes exponential technological progress and innovation. Yet, while there should be little doubt that the far-reaching advances envisioned in these approaches will play a critical role in tomorrow's military, it would not only be wrong to expect technology to be solely responsible for shaping those forces, it would be dangerous to do so. Hence, our triad—a system of systems derived from a combination of the evolutionary, penurious

robophile, and virtual trajectories described in this paper. Many of the concepts depicted in this paper are common to all three trajectories, and they are easily assimilated into the triad. Other concepts can be found in only one of the postulated futures, and those that complement each other to best address the capabilities required in 2025 have been included in the recommendations.

The ability to collect and process information will be as central to the decision-making process in 2025 as it is today, and our triad relies on significant advances in this area. As previously described, stealth and weapons technology are also expected to make significant leaps in the next 30 years. The most profound changes, though, will come with better human-machine interfaces for the commanders, planners, and pilots of 2025 which will, without doubt, improve the efficiency and effectiveness of each sortie flown. But, even with an exponential technological growth, the human in the loop and on the scene will still be a requirement. Machines can be programmed to learn; machines can be programmed to react in given scenarios; machines can make decisions. However, machines cannot be programmed with the gut feel that has always been, and always will be, an integral aspect of how we fight. As long as commonsense reasoning remains the holy grail of artificial intelligence research, the best computer available will continue to be the one between the ears. The bottom line: the counterair triad will be the right capability for performing the counterair mission in 2025, while the humans in the loop or on the scene, and their instincts and intuition concerning everything from gauging enemy intentions to the decision to fire weapons, will continue to be the last word on how we conduct the counterair mission.

# Bibliography


Barnett, Col Jeffery R. *Future War: An Assessment of Aerospace Campaigns in 2010.* Maxwell AFB, Ala.: Air University Press, January 1996.

Briefing, HQ USAF/LR to the Defense Science Board, subject: Air and Space Power Framework for Strategy Development, 19 March 1996.

Director, Test and Evaluation and Technology Requirements. "C-17 Unmanned Aerial Vehicle (UAV) Airborne Platform." *Technology Initiatives Game 95 (Systems Handbook),* U.S. Naval War College, 18–22, September 1995.

Casagrande, Wing Comdr E. E. *Non-Lethal Weapons: Implications for the RAAF,* Air Power Studies Center Paper Number 38. Royal Australian Air Force Air Power Studies Center, November 1995.

Director, Test and Evaluation and Technology Requirements. "Cooperative Air-to-Air/Air-to-Ground Engagements-Distributive Fire Control." *Technology Initiatives Game 95 (Systems Handbook),* U.S. Naval War College, 18–22 September 1995.

Director, Test and Evaluation and Technology Requirements. "Cooperative ESA Jamming." *Technology Initiatives Game 95 (Systems Handbook),* U.S. Naval War College, 18–22 September 1995.

Defense Airborne Reconnaissance Office. *1995 Annual Report: Unmanned Aerial Vehicles (UAVs).* Washington, D.C.: Office of the Under Secretary of Defense, Acquisition & Technology, August 1995.

FMFM 1, *Warfighting,* March 1989.

Fogleman, Gen Ronald R. Address to ***2025*** Participants, Air War College, Maxwell AFB, Ala., 13 February 1996.

Fulghum, David A. "International Market Eyes Endurance UAVs." *Aviation Week & Space Technology,* 10 July 1995, 40–43.

______. "Air Force Prepares New UAV Acquisitions, Operations." *Aviation Week & Space Technology,* 27 November 1995, 52–54.

______. "Predator to Make Debut over War-Torn Bosnia." *Aviation Week & Space Technology,* 10 July 1995, 47–48.

*FY96 Avionics Technology Area Plan.* Headquarters Air Force Materiel Command, 1995.

*FY96 Conventional Weapons Technology Area Plan.* Headquarters Air Force Materiel Command, 1995.

"GPS Improves Military Weapons." *Aviation Week & Space Technology,* 9 October 1995, 56–57.

Hallion, Richard P. *Storm over Iraq: Air Power and the Gulf War.* Washington, D.C.: Smithsonian Institution Press, 1992.

http://leonardo.jpl.nasa.gov/msl/Quicklooks/Pictures/iridcon st.gif, Distributed Satellite Constellation graphic courtesy of Mike's Spacecraft Library.

http://www.afit.af.mil/Schools/PA/gall3.htm, Representation of UAV Ground Cockpit and Holographic War Room graphics courtesy of Gene Lehman, AFIT/LSEC.

http://www.thomson.com:9966/janes/jpictl.html, 360 Degree Helmet Mounted Display graphic courtesy of Geoff Fowler Media Graphics © 1995.

Keaney, Thomas A., and Eliot A. Cohen. *The Gulf War Air Power Survey Summary Report.* Washington, D.C.: Government Printing Office, 1993.

Knight, Lt Comdr James Todd. "Aircraft Survivability: Vulnerability to Directed High Energy Weapons." Thesis submitted to the Naval Postgraduate School. Monterey, Calif.: Naval Postgraduate School, December 1986.

Longino, Lt Col Dana A. *Role of Unmanned Aerial Vehicles in Future Armed Conflict Scenarios*. Maxwell Air Force Base, Ala.: Air University Press, December 1994.

Mets, David R. *Checking Six Is Not Enough: The Evolution and Future of Air Superiority Armament*. CADRE Paper Special Series: The Future of the Air Force, no. AU-ARI-CPSS-91-14. Maxwell AFB, Ala.: Air University Press, April 1992.

Musashi, Miyamoto. *The Book of Five Rings*. Translated by Victor Harris. Woodstock, N.Y.: The Overlook Press, 1982.

"New GPS 2R Satellites to Operate Autonomously." *Aviation Week & Space Technology*, 9 October 1995, 54.

Shultz, Richard H., Jr., and Robert L. Pfaltzgraff, Jr., eds. *The Future of Air Power in the Aftermath of the Gulf War*. Maxwell AFB, Ala.: Air University Press, July 1992.

*SPACECAST 2020 Executive Summary*. Maxwell AFB, Ala.: Air University Press, 1993.

*Study of Oblique Detonation Wave Scramaccelerator for Kinetic Energy Weapons and Lethality Testing*. Advanced Projects Research Inc., February 1990.

Sweetman, Bill. "Major Milestones in US UAV Programme." *Interavia*, July/August 1995, 39–40.

______. "UAVs for Joint Forces." *Interavia*, September 1994, 62–64.

Szafranski, Col Richard. *GEO, LEO, and the Future*, CADRE Paper Special Series: The Future of the Air Force, no. AU-ARI-CPSS-91-2. Maxwell AFB, Ala.: Air University Press, August 1991.

***2025*** concept, no. 200006, "Unmanned Airborne Support Vehicle," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996). (PROPRIETARY)

***2025*** concept, no. 200010, "Suppression Cloud," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 200013, "Quantum Effect Communications," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 200014, "Molecular Inertial Navigation Sensor," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 200015, "Distortion Field Projector," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 200023, "Surveillance Swarm," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 900135, "Offensive Unmanned Aerial Vehicle," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 900136, "Stealthing IR Signature of Turbine Propulsion," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 900161, "Holographic C2 Sandbox," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 900172, "Miniature Precision Targeting UAV," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 900202, "Space-based Special Operations Forces," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** concept, no. 900211, "LADAR Identification Friend or Foe," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900233, "The Very Small, Very Smart Bomb," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900239, "Space-based Missiles with Photo Warheads," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900244, "Global Positioning System Guided Munitions," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900258, "Oxygen Sucker," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900278, "Real-Time Virtual Uplink with Unmanned Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900288, "Swarms of Micro-Machines," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900299, "Hunter-Killer Attack Platform," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900313, "Spaceborne/Airborne Hologram," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900317, "Tactical Information Display Helmet," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900336, "Cloaking," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900359, "Air-to-Air Missile Interdiction," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900364, "Bionic Eye," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900365, "Sensor Cockpit," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900371, "Automated Space Sentries," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900385, "3-D Holographic Battlefield Display," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900392, "Acoustic Weapon," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900405, "Weapon Health Monitoring," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900414, "Artificial Intelligence: A New Aircrew Member in Tomorrow's Combat," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900417, "Battlespace Awareness Holosphere," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900436, "Runway Targeting Smart Munition (RTSM)," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900441, "The Uninhabited United States Air Force," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).
***2025*** concept, no. 900481, "Destructo Swarmbots," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).
***2025*** concept, no. 900500, "Unmanned Fighter Bomber," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900508, "Magnetic Detection of Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900522, "Space-Based AI-Driven Intelligence Master Mind System," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900526, "Space-Based Airspace Control & Deconfliction System," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900528, "Stealthy Lethal UAV," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900550, "Personal Digital Assistant," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900554, "Adaptive Munitions," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900555, "Sensor-to-warhead Operations," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900573, "Dielectric Materials For Stealth," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900580, "In-Flight Air Refueling/Rearming of Strike UAVs," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900605, "Active Cloaking Film/'Paint'," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900619, "Panoramic Night Vision Goggles," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900638, "Autonomous Smart Bombs," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900647, "Jet Exhaust Tracking AAMS/SAMS," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900675, "Ordnance Enroute Reporting," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900676, "Defense of Missile-Delivered, Multiple Conventional Warheads," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

***2025*** concept, no. 900777, "Smart Structure Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025,*** 1996).

"UAV Force Concept." *Aviation Week & Space Technology*, 10 July 1995, 42–43.

USAF Scientific Advisory Board. *New World Vistas: Air and Space Power for the 21st Century*, Summary Volume. Washington, D.C.: USAF Scientific Advisory Board, 15 December 1995.

USAF Scientific Advisory Board. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Directed Energy Volume. 15 December 1995.

Director, Test and Evaluation and Technology Requirements. "Unmanned Tactical Aircraft Concept." *Technology Initiatives Game 95* (*Systems Handbook*). U.S. Naval War College, 18–22 September 1995.

van Creveld, Martin L. *The Transformation of War*. New York: The Free Press, 1991.

# Star Tek—Exploiting the Final Frontier: Counterspace Operations in 2025

Lt Col Robert H. Zielinski
Lt Col Robert M. Worley II
Maj Douglas S. Black
Maj Scott A. Henderson
Maj David C. Johnson

## Executive Summary

Space superiority, like air superiority today, will be a vital core competency in the year 2025. US national security is already heavily leveraged in space—a trend which will increase in the future. Likewise, other countries and commercial interests will continue to seek the valuable "high ground" of space. Where space interests conflict, hostilities may soon follow. Protecting the use of space and controlling, when required, its advantage is the essence of counterspace.

This paper demonstrates the need for, and the means by which, counterspace operations will be conducted in the year 2025. A number of factors will drive the need for a robust counterspace capability in 2025. Space will be seen as a vital national interest based on its significant role in maintaining national security. In addition, the ability to operate freely in the space theater of operations will drive the United States (US) to implement capabilities to protect its vast array of space platforms as well as those of its friends and allies. Finally, the importance of space assets in achieving information dominance will force a serious examination of the requirement for developing offensive counterspace capabilities and placing nonnuclear weapons in space.

In order to field credible and effective counterspace capabilities, the US must take advantage of current leaps in computer technologies and nurture advances in other areas. Successes in miniaturization technologies, such as nanotechnology and microelectromechanical systems, will spawn advances in space detecting and targeting capabilities and space stealth technologies. In turn, kinetic and directed energy weapon systems will likely constitute the backbone of future offensive and defensive counterspace capabilities. A counterspace architecture must and will integrate enemy target detection, target identification, command and control, defensive counterspace capabilities, and offensive counterspace capabilities to expand the options available to future commanders.

The focus we place today on counterspace requirements will directly impact the space forces we field in year 2025. This paper identifies the need for counterspace and provides a variety of concepts to do the job. Each concept includes a system description, a concept of operations, and a discussion of possible countermeasures. Finally, a systems analysis of counterspace concepts yields recommendations on key systems which should pay the greatest dividends in both the commercial and military arena. Offensive counterspace concepts recommended for future development are parasite microsatellites (robo-bugs), transatmospheric vehicles (TAV), and a ground based laser system. Defensive systems include a space interdiction net capable of detecting and intercepting satellite signals and miniature satellite body guards to protect high-value space assets. These systems will form the backbone of systems which should be pursued in order to ensure US space superiority in 2025.

# Chapter 1

# Introduction

The year is 2025. Somewhere in a low-earth orbit, a US-owned communications satellite, one of dozens, quietly and unexpectedly goes off the air. Ground controllers with their extensive computerized control systems are puzzled but surprisingly not alarmed. They should be.

Unknown to them, or to the United States (US) defense community, a consortium of rogue nation-states and organized crime cartels has just tested their new, hi-tech satellite blanker. The threat to the single satellite is formidable. The threat to US national security will be devastating when these satellite blankers can target multiple satellites simultaneously. This nightmare happens less than a year later. In an unexpectedly swift and decisive move, links to US military forces worldwide are cut, global positioning system (GPS) navigation is virtually nonexistent, and a majority of US commercial and military reconnaissance returns are nothing but static. Unfortunately, US counterspace capabilities failed in this fictional glimpse into the future.

This paper's purpose is to demonstrate the need for, and the means by which, counterspace operations will be conducted in year 2025. The future, specifically by the year 2025, will see many nations capitalizing on the vantage point of space for both commercial and military reasons. The US will continue its growing reliance on military and commercial space-based capabilities. To protect those capabilities and, when necessary, deny similar capabilities to adversaries, the US must be able to conduct counterspace operations to achieve space superiority.

In building the case for counterspace operations, we make no limiting assumptions. We expect space will be as open and accessible in 2025 as air travel is today through international airspace. The pervasive nature of space assets will foster the broad use of space by most of the nations of the world. Protecting the use of space and controlling, when required, its omnipresent potential advantages is the essence of counterspace.

This paper first frames the counterspace challenge by emphasizing the urgent and compelling need for a counterspace capability in the 2025 time frame. The discussion then turns to the road to weapons in space and the current proliferation of space capabilities today. Next, we describe counterspace system concepts that will add credibility and substance to future US counterspace operations. These concepts are organized within five technology categories: (1) space detection and targeting, (2) miniaturization, (3) space stealth, (4) kinetic energy weapons, and (5) directed energy weapons. Some concepts stretch the imagination but undoubtedly will lay a foundation for what the future space fleet should look like. Next, the concepts are woven into a space defense network to illustrate a system connectivity and concept of operations. Finally, the paper makes some investigative recommendations for future procurement and technology assessments.

# Chapter 2

# Framing the Challenge

Space superiority will be a key pillar in the war-fighting doctrine of the future. In developing joint doctrine for the twenty-first century, the Joint Warfighting Center (JWC) emphasizes the integration of three capabilities—precision engagement, battlespace awareness, and enhanced command, control, communications, computers, and intelligence ($C^4I$)—to form a "system of systems."[1] (See fig. 2-1.)

gathered in all spectra to turn battlespace awareness into knowledge. Battlespace awareness also includes information warfare. In a world heavily reliant on satellite communications, space will be a critical battlefield in any enemy's information war. Enhanced $C^4I$ will rely on space technology to identify important targets, handle data provided by the expansion of sensors, and transfer information to the weapons or

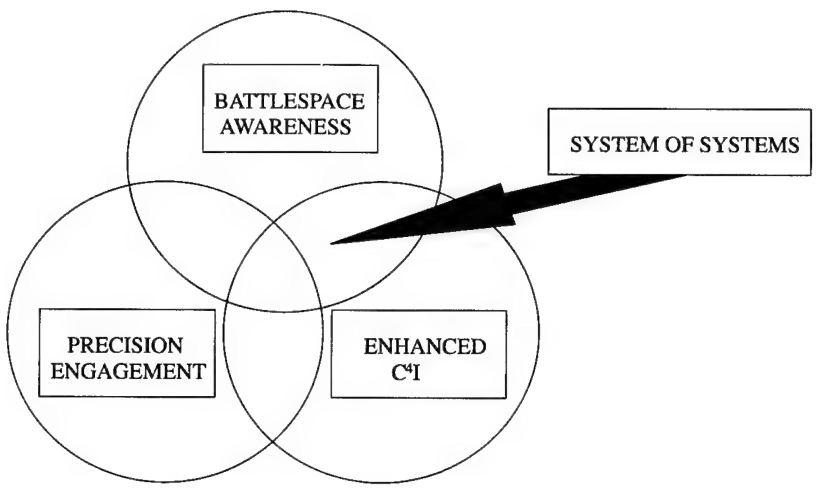



**Figure 2-1. Joint War-Fighting 2010: A "System of Systems"**

The combined effects of such future capabilities as sensor-to-shooter linkage, real-time situational awareness, precise knowledge of the enemy, exponential increases in data processing, and modern command and control systems will increase US destructive effectiveness above that of any competitor.

In the 2025 time frame, each of these capabilities could be performed solely from space, or, if not, will rely heavily on space systems. Battlespace awareness will be gained through spaceborne intelligence

forces best suited for the engagement. Precision engagement will invariably be dependent upon enhanced satellite global positioning data, space assisted targeting capabilities, and satellite communications to tell the shooter where to put bombs on target. This type of war-fighting framework will rely heavily on space capabilities. Because of this growing reliance on space, a vigorous counterspace capability will be required to protect US capabilities and deny the enemy any advantage to be gained from the employment of their space assets.

## Space as a Vital National Interest

In order to understand the importance of counterspace operations to the air and space environment in 2025, it is important to identify why space will be important to our US national interests. In addition to its role as a key enabler of future joint war-fighting doctrine, counterspace capabilities will be driven by three other significant factors in 2025. First, space will contain interests vital to US national security. Second, the US will continue to look at the freedom to operate in space just as we look at the freedom to operate in international airspace or international waters today. Third, the US will depend on unimpeded space operations for achieving information dominance.

Traditionally, the US has gone to war over only those most critical issues deemed vital interests. Historically, space has never been seen to contain such vital interests. US space systems have not yet been attacked. However, the evolution of space as a strategic necessity in the protection of US vital interests will very likely make space assets themselves vital to the protection of US sovereignty. The compelling question is, Will the US consider it an act of war if a critical space asset is intentionally degraded or destroyed in the future? As a point of comparison, Soviet space strategy envisioned space as an extension of the terrestrial and maritime battlefield.[2] As a result, any attack on their space-based warning system is a threat to which armed force, including nuclear force (if coupled with other signs of preemployment or preparation) might be the reply.[3] If the destruction of a satellite or its command and control segment leads to the loss of American lives, this should be seen no differently than the shootdown of a C-17 loaded with airborne troops. Another scenario is one in which space-based intelligence, degraded by an enemy, causes the Federal Bureau of Investigation to fail to stop a terrorist bombing which might have been avoided with unspoiled space-based information. Will this be tolerated in 2025? The ramifications of a failure to achieve and maintain space superiority are far reaching to the civilian as well as the military population.

Gen Charles Horner, former commander in chief, United Space Command, envisioned his worst nightmare as seeing an entire Marine battalion wiped out on some foreign landing zone because he was unable to deny the enemy intelligence and imagery garnered from space assets.[4] Horner emphasized the need to operate our own space systems while developing and deploying the capability to negate an adversary's use of space to support hostile military or terrorist forces. The means to accomplish these goals lie in the ability to perform the counterspace mission. Options for space system negation are bounded only by methods available to attack an enemy. Hard kill can be accomplished by directly targeting the satellite with kinetic or directed energy weapons or by attacking ground-based control facilities or launch sites. Soft kill methods include jamming or intruding the satellite signal or targeting the communication links or ground stations.[5]

In addition to protecting our satellites and denying the enemy the ability to use space against us, the US must preserve its freedom of action in space. In a future where space is equivalent to international airways or seaways of today, the US must be able to exercise an equivalent freedom of passage in space. This includes operating military and commercial satellites when and where they are needed. The increasing impact of space systems on military, political, and economic policy make the freedom to operate in this medium critical to US prosperity. Commercial interests using space today range from global telecommunications to global positioning. Ultimately, ensuring freedom of navigation to friends and allies will serve to enhance US prestige abroad in support of national security objectives. This will require the ability, through force if necessary, to assure

friendly space assets the ability to freely operate in space.

Space superiority, gained and maintained through offensive and defensive counterspace actions, supports the concept of information dominance. The main product of space systems is information. From communications to imagery, weather, or remote sensing, satellites provide information which today is used by a broad spectrum of clients. Identified as a significant part of the battlefield of the future, information warfare may be a new type of strategic warfare.[6] In the future, space will be inextricably tied to information and thus information warfare. Information dominance can mean the difference between success and failure of diplomatic initiatives, successful crisis resolution or war, or forfeiture of the element of surprise. Therefore, the ability to attain information dominance can widen the gap between friendly actions and enemy reactions. On the other hand, failure to achieve information dominance at the onset of hostilities could lead to the inability of friendly forces to conduct military operations successfully.[7] While this paper does not go into any further discussion of information warfare, it seeks to point out the value of space assets (and therefore vigorous counterspace actions) to achieving information dominance in the future.

In order to protect vital interests in space, ensure freedom of space navigation, and achieve information dominance, the US will eventually require weapons in space. The need to counter future space threats and minimize US space vulnerabilities will drive the American people to accept the inevitable—weapons in space. A discussion of the political, policy, and treaty ramifications of weapons in space will highlight some of the existing hurdles to such a venture.

## The Road to Weapons in Space

This paper proposes that by year 2025 the US, and indeed the world, will be so reliant on space systems that space superiority will be of vital importance. This in turn will require the placement of force application weapon systems in space for defense against attack and to carry out offensive actions as necessary. Many futurists, both military and civilian, have hailed the rapid development of technology and have predicted the placement of weapons in space. Many say it is inevitable. There is, however, much more to this question than technological capabilities or some kind of intuitive sense of destiny. It is a significant leap from the current political mindset about space use, to a new mindset which supports placing force application platforms in space. The obstacles to placing weapons in space lie in the following three general areas which are not mutually exclusive: international space treaties, policy, and the space sanctuary illusion.

So the question remains, What will be the road to weapons in space? What preconditions will be necessary in the areas of treaties, politics, policy, and social perspective that will lead our military and political leaders to actually break that self-imposed, invisible boundary? There are several treaties which deal with various aspects of military space activities. These include the Limited Test Ban Treaty (1963), the Outer Space Treaty of 1967, and the Antiballistic Missile (ABM) Treaty (1972). The only specific prohibition to weapons in space deals with weapons of mass destruction.[8] The current administration has been negotiating with Russia on modifying the ABM Treaty, which prohibits space-based ABM systems, in order to allow for development and deployment of more capable theater missile defense. Some say the ABM Treaty is a product of the cold war whose time has past. Others say the US should just abrogate it outright. Many are now talking about changing the treaty or abandoning it altogether. It seems possible that the ABM Treaty is on the verge of significant change which may remove one of the main treaty obstacles to force application in space.

With respect to national policy, we have come a long way from Dwight D. Eisenhower's fundamental principles that US space activity would be devoted to peaceful purposes for the benefit of all mankind. More recently, President George H. Bush's policy specified defense against enemy space attack and assuring freedom of action in space.[9] One could certainly argue that based on the changes in national policy, an important part of the "road" has already been traveled. Having a national policy that calls for force application from space is a good place to start. The problem is policy is meaningless if the nation's leaders lack the will to implement it or support those who try to implement it. Our national politicians need to recognize the critical nature of space systems, space vulnerabilities, and the need to support pursuing space control and force application capabilities in space. This awakening must occur before a crisis arises and before an antagonistic nation either attacks or deploys the capability to destroy US space assets and holds the nation hostage. Shifts in political will may be forming today as the Congress has been trying to pass legislation to deploy a national missile defense system.

Public will is another matter and is something infinitely difficult to assess. Focusing closer to home, the American people must be asked, "Are you comfortable with the idea that some rogue nation is able to destroy both military and civilian satellites causing you to lose your cable TV, your cellular phone, and the navigation system that guides you to your favorite fishing hole?" All things considered, it seems reasonable to predict by 2025 the US will have mustered the political and social will, in recognition of the absolute criticality of assured freedom of operation in space, to get over the sanctuary hurdle and place the necessary space force structure in place.

## The Growing Need for Counterspace Capability

In order to understand why a counterspace capability will be critical in 2025, it is only necessary to look at recent developments which point to the explosive growth in usage of space assets worldwide. As both commercial needs and military missions are increasingly met via space systems, the ability to protect the sovereignty of US and friendly satellites will grow in importance. Make no mistake—there is a potential threat. With the intent to "deny the use of outer space to other states," the former Soviet Union developed and tested antisatellite (ASAT) weapons in the 1960s and 1970s.[10] Moreover, a stated high-priority Soviet objective in the late 1980s was a space-based high-energy laser ASAT weapon to complement their current ASAT capable systems.[11] Based on these developments, it is reasonable to assert that a number of nations will develop an ASAT capability over the next 30 years.

## Proliferation of Access to Space Systems

### United States

The US is critically dependent on space. Communication, navigation, intelligence gathering, and weather observation are just a few of the areas in which the US has leveraged its future into space. This investment vigor extends to the commercial arena as well. Numerous domestic and international businesses have committed large sums of capital in order to deliver products and services to the customer. According to the *New World Vistas: Space Applications Volume*, in the commercial telecommunications area alone, six different constellations will become operational in the late 1990s (table 1).[12]

In addition to the explosive commercial growth in space, the military continues to press the strategic advantage that control of the space domain offers. Desert Storm can arguably be designated the "First Space War." From weather forecasting to target intelligence, US success relied heavily on spaceborne systems. National assets, combined with our GPS constellation, increased

**Table 1**

**Proposed LEO Communications Systems**

| | COMPANY | # SATELLITES | ORBIT/ INCLINATION | COST | IOC |
|---|---|---|---|---|---|
| TELEDESIC | MICROSOFT/MCCAW | 900 (40+4 IN EACH PLANE) | 21 PLANES 98.2 DEG SUN SYNC | $15B | 2001 |
| IRIDIUM | MOTOROLA, LOCKHEED | 66 (+ 7 SPARES) | 6 PLANES/11 EACH | $3.4B | 1994 |
| GLOBAL STAR | LORAL, QUALCOM & SPACE SYS | 48 (6x8) +8 SPARES | 8 PLANES 52 DEG | $1.8B | 1997 |
| ELLIPSO | ELLIPSAT CORP/ WESTINGHOUSE FAIRCHILD | 14–18 | ELLIPTICAL 63.4 DEG | $650M | 1998 (?) |
| ODYSSEY | TRW | 12–15 | 55 DEG 3 PLANES 4 SAT | $1.3B | 1999 |
| ARIES (FORMERLY) | CONSTELLATION COM, INC. & DEFENSE SYSTEMS | 48 (4x12) | 4 PLANES CIRCULAR | $300M | 1994 |

**Source**: USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the space applications volume, 15 December 1995), 7.

the accuracy of our forces, both in, and out of the Kuwait/Iraq theater. The defense satellite program (DSP) system provided tactical warning of Scud launches within minutes, enabling our defense forces to come to their highest alert and defeat the threat. More so than in any past conflict, connectivity between the fielded forces and the commander make information and decisions instantly available to the one who needed it most—the war fighter. As the US depends more and more on precision as a force multiplier, the ability to detect, identify, and target threats will become paramount. To counter increasingly mobile enemy forces, this ability needs to be either real time or near real time. Space offers a medium for near instantaneous, cheap communications. It offers the possibility of continuous surveillance plus highly accurate positioning. In Jeffery Barnett's book, *Future War*, he called these "war-deciding capabilities."[13] As such, our space capabilities must be protected and the enemy's capability must be negated.

### The "Rest" of the World

Other economic and military powers also recognize the value of space. The European Community, the Commonwealth of Independent States, Japan, and China, just to name a few, all have active launch programs deploying assets into space. While our future quarrel may not be with the "owner" of the space asset, the enemy's ability to access the information could be very detrimental to our cause. Even in 1991 the "CNN factor" was significant. Saddam Hussein certainly had his television on, even if he could not talk to his troops.

The Teal Group Corporation, a defense and aerospace analysis firm, identified 949 spacecraft that have been funded or scheduled for launch from 1995 to 2004.[14]

It is likely that the end of defense export restrictions on sales of computers will allow many countries to manipulate, store, and disseminate medium-resolution data, such as that offered by satellite positioning and tracking (SPOT) and LANDSAT, and make the imagery vastly more useful to foreign militaries. By encouraging US concerns to become commercial leaders in selling imagery as fine as one meter resolution, the government hopes to discourage many other nations from developing their own systems or buying services elsewhere.[15]

These current capabilities, demonstrated by multiple countries, are a loud warning to the US to maintain its edge in space technology. Improved capability can be expected in the future. The increase in satellite information vendors means organizations without space capability can purchase the end product from a wide variety of sources.

## System Vulnerabilities in 2025

Most, if not all, space systems have three segments: space, ground, and user. Using a communication satellite system as an example, the space segment is the actual satellite. The ground segment likely consists of one or more stations that control customer access to the satellite. The user segment is the customer, the person who is trying to communicate, as well as any user equipment.

Each segment has its own vulnerabilities in a combat environment. Capabilities described later in this paper may make satellites the most lucrative targets to attack, while the political situation may make such an attack untenable. The US may be able to strike a satellite system because it is supplying a third country with intelligence, but unwilling to do so because we are engaged in talks of a delicate nature over a separate issue. Using the same rationale, the ground segment may be too politically sensitive because of its location. In reality, the user segment may be the most politically acceptable target, but it is practically invulnerable due to its dispersed nature.

Existing US technology can strike all segments of space assets. Demonstrated F-15 (ASAT) takes low-earth-orbit systems targets today.[16] Extensions of this, and other technologies discussed later, will make medium earth orbit and high earth orbit systems vulnerable in 2025. Ground and user segments today are vulnerable to both conventional and nonconventional attack.

## Threats to Space Systems in 2025

There will be multiple threats to space-based systems in the future. Some will involve threats to the space segment, some the ground, and some the user. These threats could or will come from current conventional forces, space-based forces, or other advanced technology ground/air forces. These threats can be extensions of today's technology, such as F-15 ASAT derivatives or the detonation of nuclear weapons in space. Another possibility will result from leaps in technology that enable realistic directed energy, kinetic energy, and electromagnetic pulse based weapons to be directed to individual targets.

To this point, the discussion has focused on the need for counterspace capabilities in 2025 and the challenges facing US forces in gaining and maintaining space superiority. The next section describes key technology areas, ranging from space detection and targeting to directed energy weapons, as well as specific concepts and capabilities, which will enable US commanders to absolutely control the high ground in 2025.

### Notes

1. Joint Warfighting Center Doctrine Division, "Warfighting Vision 2010" (draft) (Fort Monroe, Va.: 1995), 10.

2. Gen John L. Piotrowski, "A Soviet Space Strategy," *Strategic Review*, Fall 1987, 56.

3. Ibid., 57.

4. Prepared statements of Gen Charles Horner, commander in chief, United States Space Command, in Senate, *Space Seen as Challenge, Military's Final Frontier* (Defense Issues, Prepared Statement to Hearings before the Senate Armed Services Committee, 90th Cong., 1st sess., 1993), 7.

5. Ibid.

6. Barry R. Schneider, "Battlefield of the Future," in *The Revolution in Military Affairs* (Maxwell AFB, Ala.: Air University Press, 1995), 80.

7. Maj James G. Lee, *Counterspace Operations for Information Dominance* (Maxwell AFB, Ala.: Air University Press, 1995), 4.

8. AU-18, *Space Handbook*, vol. 1, *A Warfighter's Guide to Space* (Maxwell AFB, Ala.: Air University Press, 1993), 55–56.

9. Ibid., 103.

10. Nicholas L. Johnson, *Soviet Military Strategy in Space* (New York: W. W. Norton and Co., 1986), 155.

11. Capt Gregory C. Radabaugh, "Soviet Antisatellite Capabilities," *Signal*, December 1988, 81–83.

12. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the space applications volume, 15 December 1995), 7.

13. Jeffery R. Barnett, *Future War, An Assessment of Aerospace Campaigns in 2010* (Maxwell AFB, Ala.: Air University Press, 1996), 41.

14. James R. Asker, "Space Control," *Aviation Week & Space Technology*, 23 May 1994, 57.

15. Ibid., 51.

16. While the technology demonstration program validated the concept, F-15 ASAT missiles and warheads were not maintained after cancellation of the program.

# Chapter 3

# Key Technologies and System Descriptions

## Space Detection and Targeting

### General Discussion

The linchpin in delivering a critical blow to an enemy system anywhere in the expanse of the air and space environment is accurate detection and targeting. This capability is crucial in providing total battlespace situational awareness. To make this happen, significant advances are required in radar, laser, and infrared detecting and tracking technologies. While "detecting and targeting" imply offensive capabilities, they also lead to formidable defensive capabilities in countering enemy kinetic energy weapon (KEW) and directed energy weapon (DEW) attack.

In order to defend against an ASAT, for example, the defending satellite (or its controlling system) must be able to detect approaching threats in order to defensively react. Defensive traits must go beyond today's satellite hardening and limited space maneuvering. In 2025, space systems must be able to organically detect intruders, have built-in stealth characteristics, and if needed, be able to actively defend against attack. The following concepts explore some system possibilities intended to give the space force commander dominant battlespace awareness.

## Gravity Gradiometer

### System Description

Gravity gradiometers are instruments and systems that detect mass density contrasts (fig. 3-1). Recent gravity gradiometer research has focused on sea-based submarine detection applications.[1] This concept goes several leaps forward and proposes its use in space as a passive detection system.

### Concept of Operations

With multiple gravity gradiometers located on multiple satellites in orbit, approaching "foreign bodies" can be passively detected. Data and measurements gathered could be combined with data from other detection devices in Kalman filtering or data fusion algorithms to enhance detection and even identification probabilities.

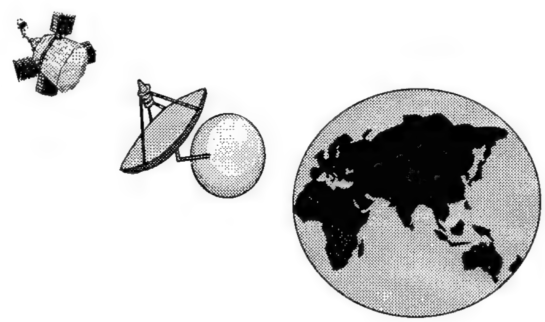


**Figure 3-1. Gravity Gradiometer**

Gravity gradiometers embedded in multipurpose satellites or spacecraft will detect approaching bodies. Multiple gradiometer systems can accurately pinpoint foreign body locations for follow-on defensive reactions.

Four critical subtechnologies are identified for feasibility investigations with gravity gradiometers. These are (1) gravity gradiometer technology itself; (2) advanced filtering algorithms to combine data from other sensors to enhance detection, location, and identification of approaching bodies; (3) modeling capabilities to appropriately model gravity gradiometer errors and signals; and (4) simulation capabilities to determine the gravity gradiometer accuracy required as a

function of the size and mass distribution of the body under scrutiny, as well as its proximity and maneuver pattern. In order to be able to use the gravity gradiometer in a space detection mode, technology advances must yield a system, which can be deployed in space, capable of detecting an object on the order of 100 kilograms at a range of 100 nautical miles. Reaching this sensitivity by 2025 is an extreme challenge and may be a limiting factor in fielding this technology.

#### Countermeasures

Synthetic gravity fields may provide effective countermeasures to gravity gradiometer systems. However, the technological leap to "produce" gravity is formidable and not likely by the year 2025. Nonetheless, combining data from other sensors (space based or ground based) to validate organic gravity gradiometer inputs would counter synthetic gravity deceptive attempts.

### Anti-ASAT System

#### System Description

The Anti-ASAT system incorporates a host of sensors embedded on orbiting satellites or spacecraft combined with an artificial intelligence program to detect approaching bodies.[2] Sensors will detect all forms of radiated wave energy (IR, RF, electromagnetic, etc.). Additionally, the concept design includes ablative and reflective coatings on the host satellite for defense against directed energy attack (fig. 3-2).

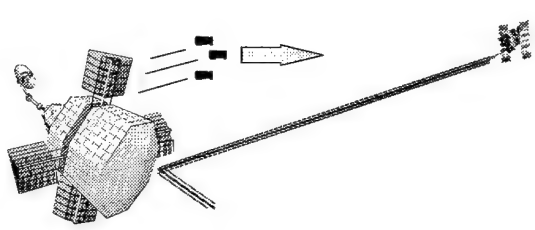


**Figure 3-2. Anti-ASAT System**

#### Concept of Operations

This is a satellite self-protection system. If the satellite or spacecraft is approached or attacked by external threats, onboard protective systems eject matchbox-sized "defenders" to home on the intruder, attach to it, and disable it with shaped charges or degrade it by leaching power or disrupting uplink/downlink commands. Hypothetical design should provide a probability of survival ($P_s$) of .7 against co-orbital threats, .4 against impact or ASATs, and .25 against energy beams. When placed on stealthy satellites, a measure of stealthiness is lost although $P_s$ increases to .9 against co-orbital ASATs and .6 for impact or ASATs and energy beams.[3]

#### Countermeasures

An overwhelming attack could defeat the system's self-protection capabilities and destroy or degrade the satellite.

### Space Interdiction Net

#### System Description

Key to any counterspace operation in the future will be total battlespace awareness. The purpose of the space interdiction net is to detect satellite transmissions, identify the source of those transmissions, and find the end user of the information (see fig. 3-3).[4] This capability is required in order to selectively deny information to an adversary from his own military satellite system or a commercial system. In addition, a space interdiction net will be used to determine whether damage to US or friendly satellites is a result of malicious action or natural causes, such as solar flare or asteroid collision. Consisting of an orbiting grid of satellites capable of continuous coverage of the earth, the space interdiction net will use a web of interlinked microsat systems to radiate a very low power force field over the globe. The field generated by the constellation will act as a blanket around the earth and will be able to detect any

energy penetrating the blanket, seek out the desired signal, and jam or degrade that portion of the signal which is important. This force field will be capable of picking up transmissions in a wide range of frequencies and will use triangulation from three or more satellites to pinpoint the source. A capability to detect 70 percent of the transmissions will probably be attainable in 2025. All data deemed not critical to enemy hostile action is left alone to be received as originated. This selectivity enables US commanders to take positive military action to deny an enemy critical information without disrupting nonmilitary information traffic.

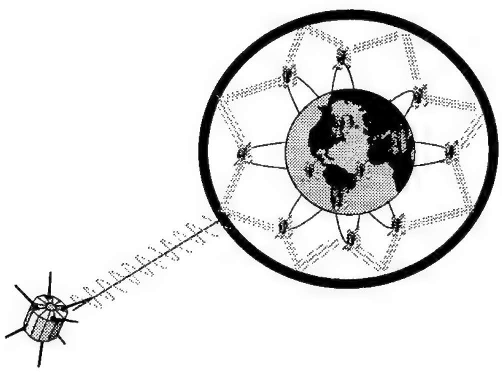


**Figure 3-3. Space Interdiction Net**

In 2025, the number of satellites orbiting the earth will rise dramatically (increasing by 25 percent between 1999 and 2005)[5] and commercial systems will form the backbone of the space information network. The key to performing counterspace operations in this environment will be the ability to identify the critical information being transmitted to an enemy. Upon detection of hostile satellite signals, the interdiction grid will be able to deploy a number of countermeasures ranging from jamming and electronic warfare to destruction via kinetic or directed energy weapons. These actions ultimately keep the end user from capitalizing on critical information from his spaceborne assets.

From a technology standpoint, the power source for this system of integrated sensor network is the most daunting challenge. Battery technology may not advance enough by 2025 to provide continuous power to the system. Solar power can be used a majority of the time, but battery technology is still required for times when sensors are out of view of the sun. A possibility is to use a thin film reflector on orbit to light solar cells on the sensor satellites as they orbit in the shadow of the earth (see the solar optical weapon concept presented later in this paper).

As shown by a variety of concepts presented in this paper, there are a wide variety of ways to disrupt, deny, degrade, or destroy satellite transmissions at the source. However, these methods are not selective in that they deny information to all users. The detection and interdiction system will be capable of specifically identifying only that information which is being used against the US or its allies. This information can then be used by field commanders and the national command authorities (NCA) to determine whether or not to take action against the satellite itself or its owners. In many cases, the "owners" will be known, as in the case of multinational corporations who operate satellites as part of their business infrastructure. Again, the spectrum of options ranges from soft kill to hard kill.

Another particularly interesting possibility is the modification of the ionosphere to disrupt communications. A number of methods, such as chemical vapor injection and heating or charging via electromagnetic radiation or particle beams, have been proposed to modify the ionosphere.[6] Because ionospheric properties directly affect high-frequency communications, an artificially created ionization region could conceivably disrupt an enemy's electromagnetic transmissions. Offensive interference of this kind would likely be indistinguishable from naturally occurring space weather. The capability to create ionization regions could also be used to detect and precisely locate the source of transmissions.

In order to interdict specific signals, the space interdiction net will be capable of projecting a force field between the target and the receiver. This force field will be in the form of a magnetic field or charged particle cloud. Another possible means of surgically removing specific transmissions is a precision molecular particle which, using a nanotech computer brain, follows the data stream to the source. Once at the origination point, the smart particle destroys the frequency bandwidth on which the critical data is being transmitted. We recognize that technology to dissect transmissions at the molecular particle level may not be achieved by 2025 but once achieved will add dramatic leap in counter-space capabilities.

This concept relies on a tightly integrated net of satellites operating in low-earth orbit (LEO). The system must be placed in a roughly 250–300 nautical mile orbit in order to be able to detect transmissions from major orbital regions from low earth to geosynchronous. In order to provide continuous coverage to all points on earth, the system will consist of three interlinked constellations of 66 satellites for a total of 198 satellites. All satellites will be interlinked with each individual satellite capable of assuming control of a "hot" sector, one in which hostile transmissions are detected. Satellites will consist of a power system and phased array antenna to project the low energy detection field. In addition, a very high-speed computer will integrate the incoming detection data and correlate the data to a source through triangulation. Finally, a directional antenna, on order from the command and control subsystem, will project a controlled cloud of charged particles to a point in the sky. The end result is a large charged particle cloud or ionization region placed precisely between the sender and receiver. A further leap would use molecular sensors and computers to lead individual molecules in the charged particle cloud to seek out and destroy specific bits of information from the data stream. The idea of surgical strike has now been taken to the molecular level.

The limiting factor in making the space interdiction net a reality will be the ability to project low power fields over large areas in space. A number of evolutionary advances in space weather forecasting and observation are required to make ionospheric exploitation a reality. The high-speed computer technology necessary to control the smart particles should be available in 2025. In addition, nanotechnology computers may make possible the development of smart charged particles which will be capable of finding and destroying signals. The combination of very low orbits (prone to orbital decay) and the high number of satellites required to form the system will drive the need for a very high resupply rate. This in turn points to the need for a very robust launch capability.

**Concept of Operations**

The space interdiction net will be in constant orbit around the earth. The system will monitor space transmissions continually while especially looking for strategic indicators which may be warning of impending escalation. With the capability to perform selective offensive counterspace, the activation of the system itself can act as a deterrent to further aggression. Intelligence inputs will give the system an initial estimate of enemy space capabilities which will enable the detection and interdiction system to focus on certain satellite constellations.

The grid will be capable of interrupting key information from all types of satellites including communication satellites, imagery satellites, and weather satellites. It will be closely integrated with the $C^4I$ system to allow commanders at all levels near instant data on which enemy capabilities have been negated. In addition, the grid will be linked to the other assets which makeup the counterspace system. If precision signal blocking is not necessary, alternate counter-space systems such as directed energy or parasite microsatellites (described later as robo-bugs) can be employed to disrupt or

destroy the enemy's space capability. In order to ensure the grid is constantly maintained, a number of on-orbit spares will be placed in parking orbits to be used as needed. A quick-turn launch capability is required to keep the system operationally ready due to expected orbital decay of the LEO satellites which makeup the system. The interdiction net must be capable of integrating with the command and control system as well as the intelligence system.

### Countermeasures

An important countermeasure to this type of system lies in the ability to disrupt or create holes in the detection field. Encryption methods may be capable of making signals hard to attack with smart molecular munitions. If the sender can disguise transmissions or make them capable of changing while en route to the receiver, it will be difficult to identify and attack the right data. Maybe the simplest way to defeat this type of system would be through redundancy via the proliferation of small satellites capable of performing specific missions. Thus, if one system is detected and jammed by the interdiction net, the mission can be accomplished by any number of other satellites capable of transmitting the critical information. This method also complicates the ability to target systems by increasing the cost associated with disrupting or negating a large number of miniature systems operating over a vast battlespace. Should ionospheric disruption become a reality, it could be turned against the space interdiction net to disrupt the low power field or interrupt essential command and control functions.

## Miniaturization

### General Discussion

Miniaturization is about the age old quest to do more with less, in military parlance, to package more capability in a smaller package. In space, the main reason for miniaturization is weight savings—the ability to maximize precious spacelift resources. This in turn reduces the cost of space systems. Another reason for miniaturization in space is redundancy. A constellation of small satellites performing parcels of the mission is not so vulnerable as a mega-satellite tasked with doing it all. Finally, miniaturization in space opens up new avenues to exploit enemy space systems. It is in this realm that miniaturization can make a true contribution to the counterspace mission. Of note is the urgent desire for commercial industry to exploit miniaturization. Dr Tom Velez, in the keynote address at the eighth annual American Institute of Aeronautics and Astronautics (AIAA) conference on small satellites noted that the small satellite or "smallsat" industry is growing "for reasons that are not political, not military, not scientific, but commercial . . . they're cheaper and more capable of providing user services."[7] This commercial interest should aid immeasurably in the development of technologies and systems that will enable a robust counterspace capability in 2025.

The electronics industry has shown the ability to double the number of transistors on a microchip every 18 months. This trend has driven a dramatic revolution in electronics. Researchers note that the ability to "manufacture millions of microscopic elements in an area no larger than a postage stamp" has inspired further miniaturization technology.[8]

Two emerging technologies show particular promise in making spacecraft smaller and more capable. The first, microtechnology, is the combination of miniaturized mechanical and electric components in microelectromechanical systems (MEMS). The Scientific Advisory Board's *New World Vistas Space Technology Volume* report labels MEMS as the next step in the microelectronics revolution in which multiple functions are integrated on a microchip.[9] An example of a future MEMS is on-chip optics which will be used to provide agile target recognition and tracking.

The second technology, nanotechnology, is not nearly as developed. Its chief proponent, Eric Drexler, describes it as "taking what we're very familiar with on a macroscopic level and doing that on a vastly smaller scale using the basic building blocks of matter."[10] Drexler notes that instead of taking something large, like a silicon wafer, and making it small, nanotechnology starts with molecules and atoms and builds up in Tinkertoy fashion. The results will go far beyond simply making atom-scale computers. The *New World Vistas Materials Volume* report notes nanobased processing could provide advanced electro-optical materials, molecular scale sensors, and dynamic stealth materials.[11]

Nanotechnology offers the capability to build molecule-size factories capable of churning out thousands of specialized nanomachines. Researchers estimate that it will take 20 to 30 years to achieve practical nanotechnology results. The following section describes the link between advances in miniaturization and proposed systems to perform the counterspace mission. Two counterspace concepts with miniaturization as the key enabling technology are promising. Satellite bodyguards—fleets of small satellite sentries—will protect high-value space assets (fig. 3-4). Robo-bugs—parasite microsatellites capable of operating on or near enemy satellites—will use jamming and electronic warfare methods to disrupt and degrade information transmitted from enemy space systems. A description of these potential systems along with a proposed concept of operations follows.

## Satellite Bodyguards

### System Description[12]

In the years 2000–2005, we can expect a rapid growth in the average number of payloads being launched annually.[13] The decades following that will probably see launch rates grow at a much steeper rate. In

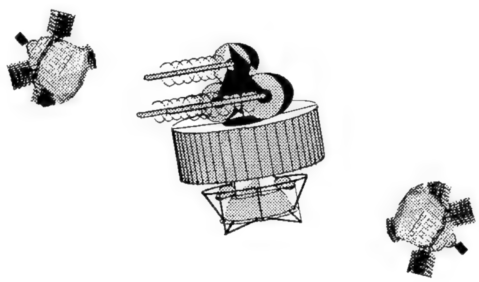


**Figure 3-4. Satellite Bodyguards Protecting a High-Value Space Asset**

order to protect the vast number of high-value space assets orbiting in 2025, active defensive systems must be able to respond to a wide range of threats. One way to meet this challenge is to place a large fleet of satellite bodyguards in orbits containing critical US and allied satellites. The large number of satellites requiring protection will drive an equally large constellation of bodyguards capable of performing a wide variety of functions. The most efficient means of achieving such a goal is to pursue advances in miniaturization such as microtechnology and nanotechnology.

A space-based satellite bodyguard system might consist of an integrated network of orbiting microsatellites each performing specific subsets of the space protection mission. Similar to P-51 fighter aircrafts flying escort for B-17 bombers in World War II, this system of satellites will be required to detect enemy presence, determine the threat, and act to defeat the threat. However, the bodyguard system of 2025 must take this idea one step further and capitalize on miniaturization to make bodyguards weight- and cost-effective. The best way to accomplish this is through what Col Richard Szafranski and Dr Martin Libicki, air and space visionaries, call a meta-system.[14] A meta-system is composed of individual systems working together to perform such tasks as information collection, battlespace awareness, and interfacing with other components of the cooperative distributed network.

Key components of any such meta-system will be miniature sensors coupled with high-speed computers to integrate inputs from multiple bodyguards. The sensor array (an integrated net of sensors on a number of distributed bodyguards) must be capable of detecting inbound threats operating in any spectrum including radar, infrared, acoustic, and visual. Current advances in smart materials and nanotechnology, as well as the miniaturization of high-speed computer technology, will make such a system feasible in the 2025 time frame. This is supported by the trends in computer chips which have gone from circuits three microns wide 10 years ago to current machines which are fabricated at the .35 micron level. Ralph Merckle of Xerox predicts the mainframe of the first or second decade of the twenty-first century "will be the size of a sugarcube and will execute more instructions per second than today's Cray supercomputers."[15]

While miniature high-speed computers and intelligent materials will increase the capabilities and staying power of the satellite bodyguard, advances must also be made in power and propulsion. Possible solutions to the power problem are nuclear batteries, advanced solar batteries, or fusion technologies, each resulting in a virtually inexhaustible fuel supply. Advances in nonchemical high specific impulse propulsion techniques may provide the revolutionary leap in propulsion needed to make a bodyguard capable of high-speed maneuvering (satellite jinking).[16]

A large fleet of bodyguards will be required to form a meta-system capable of protecting the growing number of high-value space assets, both military and commercial. This system, coupled with the need to launch large numbers of dispersed bodyguards in order to reduce the system's vulnerabilities, will make miniaturization a crucial technology in 2025. A robust space launch infrastructure as well as rapid resupply capability is necessary to keep a satellite bodyguard system operational in a high-tempo environment.

### Concept of Operations

In applying the meta-system concept to a satellite bodyguard system, individual bodyguards the size of a laptop computer will perform unique subsets of the overall mission. Based on the same basic design, some bodyguards will be tasked as sensors with the mission to identify and track possible threats. Other bodyguards will be assigned a defensive role where their main function is to seek out threats and negate them. Taking this one step further, defensive bodyguards may be active or passive. Active defenders will use high-specific impulse propulsion techniques (such as electrostatic, electrothermal, or electromagnetic systems which use electric power to accelerate propellant gasses to high exit velocities) to seek and destroy a space-based threat.[17] Passive defenders will use smart materials (capable of adapting to deflect or absorb inbound energy) to minimize electromagnetic or directed energy damage to a high-value asset. In a worst-case scenario, the bodyguard will sacrifice itself to protect the high-value asset it is guarding. Other bodyguards will be outfitted to perform critical computing and fire control functions.

For incoming ASAT missiles, the system may relay position, velocity, and acceleration data to an orbiting directed energy system which will make the kill. Another option is to equip bodyguards with satellite protective armor which would respond to a KEW attack much as today's reactive tank armor responds to antitank fire.[18] An alternate mission for a satellite bodyguard employs electronic warfare to confuse the enemy. Equipping bodyguards with electronic signals duplication capability will enable a bodyguard to replicate the electronic signature of a high-value asset.[19] By saturating the battlespace with large numbers of small and cheap bodyguards (which to enemy sensors appear to be high-value satellites), the problem of finding and destroying the

truly critical satellite becomes much more difficult for an enemy.

Due to the high-risk mission they perform, satellite bodyguards will likely require steady replenishment through the logistics system. Self-replicating nanotech systems may aid in the rapid replacement of damaged bodyguards. A command and control link is assumed to be in place and is critical to the satellite bodyguard concept.

### Countermeasures

One way to counter a satellite bodyguard system is to saturate the battlespace around the high-value system with threats to overwhelm the bodyguard meta-system. However, proliferation of inexpensive bodyguards performing subsets of the overall mission may make shooting them too expensive for a future adversary. The command and control function may represent the center of gravity of an integrated meta-system. Destroying the command and control link will effectively disable the bodyguard system by negating the critical integration of information between bodyguards. A hardened burst transmission send and receive capability will decrease the vulnerability of the communications link. Finally, the idea that visibility (to enemy sensors) may equate to death in 2025 makes emission control of vital importance to satellite bodyguards. Stealth as well as minimum communication requirements will help to make bodyguards more survivable in the battlespace of the future.

## Robo-Bug

### System Description[20]

In his 2,500-year-old classic *The Art of War*, Sun Tzu states that "all warfare is based on deception."[21] Those words continue to ring true today in the realm of space warfare. The idea of a robo-bug is to use small satellites, equipped with stealth or cloaking capability, to get close to a target enemy satellite. The robo-bug will then take on characteristics of the target. A plausible scenario has an undetected robo-bug satellite affixing itself to a navigation satellite similar to the global positioning system (GPS). The robo-bug will have the capability to detect when a satellite is providing information to an adversary. At the right time, the robo-bug is activated and begins to disrupt the signal through jamming or other electronic warfare methods (fig. 3-5).

**Figure 3-5. Robo-Bug Microsats in Action**

Another option is to attack the link system, described as the electromagnetic energy used for space system uplink, downlink, or cross-link. Given a link segment made up of electromagnetic energy, the primary technology used to attack the link is electronic warfare in the way of jamming or spoofing. Jamming is transmitting a high-power electronic signal that causes the bit error in a satellite's uplink or downlink signals to increase, resulting in the satellite or ground station losing lock.[22] Spoofing involves taking over a space system by appearing as an authorized user. An example is establishing a command link with an enemy satellite and sending anomalous commands to degrade its performance. Spoofing is one of the most discreet and deniable nonlethal methods available for offensive counterspace operations.[23]

In his work on counterspace options, Maj James Lee presents a number of options which can be used in an offensive counterspace mission against a peer competitor. These options target the entire system (ground, link, and orbital segments) and range from nonlethal disruption to hard kill as listed in table 2.[24] A robo-bug system will be capable of performing the entire spectrum of offensive counterspace options.

**Table 2**

**Offensive Counterspace Options**

| | PEACE | CRISIS | WAR |
|---|---|---|---|
| **GROUND SEGMENT** | | | – NONLETHAL WARFARE<br>– STRATEGIC ATTACK<br>– SPECIAL OPS |
| **LINK SEGMENT** | – LOCAL JAMMING<br>UPLINK<br>DOWNLINK | – LOCAL JAMMING<br>UPLINK<br>DOWNLILNK<br>– SPOOFING | – JAMMING<br>UPLINK/DOWNLINK<br>– SPOOFING |
| **ORBITAL SEGMENT** | – NONLETHAL<br>DISRUPTION | – NONLETHAL DISRUPTION<br>– MISSION KILL | – NONLETHAL DISRUPTION<br>– HARD KILL/MISSION KILL |

**Source**: Maj James G. Lee, *Counterspace Operations for Information Dominance* (Maxwell AFB, Ala.: Air University Press, 1995), 34.

The robo-bug is capable of destroying the enemy satellite with a shaped charge explosive or high energy event such as high-power electromagnetic pulse (EMP) or high-power microwave burst. An alternative, the ability to accomplish the counterspace mission with what General Horner, in a speech to the Senate Armed Services Committee on 22 April 1993 described as a "soft kill" (including jamming or intruding the satellite signal and communication links) enables US forces to deny an enemy use of space information without destroying satellites. In a future which sees a blurring of space missions between military, multinational corporations, and numerous governmental organizations, this capability will offer the commander a desirable option to be used in meeting a politically sensitive military objective—space superiority.

A robo-bug system will be comprised of a main module which will take care of basic needs such as power, navigation, and station keeping. The satellite itself will be built using stealth cloaking techniques (described later in this paper). The command and control system will be used to receive direction via ground or space link and act upon that information to direct the robo-bug to its assigned target. The heart of the system will be the payload which will have a specific mission. Missions are discussed in the concept of operations. The emerging technologies which might make a robo-bug system feasible are MEMS technology, nanotechnology, and small high-speed computing. As previously discussed, each of these technologies show signs of being near maturity in the 2025 time frame.

### Concept of Operations

The idea of a robo-bug is not to act as an antisatellite weapon. Instead, the robo-bug uses electronic warfare methods to negate a satellite's capabilities without permanent damage. Robo-bugs will be pressed into operation early in a potential conflict to degrade or eliminate the detection, imagery, and communications capabilities of an adversary.

Robo-bugs must operate in such a manner as to make any loss in enemy satellite fidelity very subtle so the likelihood of discovery by the operator is as small as possible. This can be done in a variety of ways. In addition to the spoofing mission as described in the navigation satellite example, another possible mission (forwarded by Gen Charles A. Horner) is jamming or intruding the satellite signal or targeting the satellite communication links. This negates the enemy's ability to maneuver the satellite or

to deploy onboard systems such as sensors and antennas. Yet another possible mission is to simply act as a power drain, sapping the power from the enemy satellite much like a tick on a dog.

### Countermeasures

In their paper "Tactical Deception in Air-Land Warfare," Charles Fowler and Robert Nesbit make a fundamental observation that "the military group that is not devoting appropriate efforts to include tactics, R&D, and plotting and scheming in general for deception is almost certain to be vulnerable to being deceived itself."[25] Any future US space system must be capable of defeating an enemy parasite system. Specific countermeasures to a robo-bug system are based on the ability to detect disruption efforts and take action. Assuming they can find a robo-bug, an enemy might do periodic maneuvers to avoid it or take offensive action to destroy it. Deception may also be an effective method of countering a robo-bug system. If a satellite is able to radiate emissions which make it appear to be nonthreatening (or even appear to be a friendly satellite), it may be able to fool a robo-bug.

Another very effective method in countering a parasite system is dispersion—using large numbers of small satellites to overwhelm detection and targeting systems. This method causes the enemy to expend numerous resources in an attempt to protect his valuable space systems. Once an enemy suspects a satellite is being influenced by an unfriendly parasite, confirmation can be made by comparing data to known values. However, without a way to rid itself of the robo-bug, the satellite may very well be rendered useless. Once again, the command and control link between the commander and the robo-bug presents a vulnerability. The ability to operate in a secure command and control environment continues to be an essential part of any counterspace concept.

## Space Stealth

### General Discussion

Stealth conjures up images of a strike package of aircraft operating deep in enemy territory while the adversary waits, watches, and listens, all to no avail. Author J. Jones describes stealth as the act of proceeding furtively, secretly, or imperceptibly.[26] Fast forward the year to 2025 and imagine an enemy hunter-killer satellite team cruising right past a US command and control platform without the faintest hint of detection. Stealth, defined in terms of revolutionary molecular technologies, can be a key component in the protection of friendly space capabilities against enemy attack—classical defensive counterspace.

To date, numerous passive measures such as hardening, redundancy, and cross linking have served to protect US satellites from threats in space. Our status as the lone superpower and leader in space has meant these threats have so far been very benign. On the other hand, the future will likely hold greater threats both in number and sophistication. By taking a significant technology leap, we can defeat these future threats. This leap is broadly categorized as space stealth or cloaking. In essence, we are talking about making satellites invisible.

Most people are familiar with the stealth concepts employed on modern day aircraft such as the F-117 and the B-2. Current stealth technologies seek to blend signature reduction techniques in the radar, infrared, visual, and acoustic domains.[27] The classical design problem has been balancing aircraft designs to minimize the signature in each domain. Unfortunately, this does not lead to an optimal solution. For example, highly reflective materials are ineffective in a visual or radar environment but are very desirable in an infrared environment. In 2025, standard detection methods as well as a number of new and unique methods will have to be countered in order to achieve true stealth. The

technological leap that may enable us to do this is satellite cloaking.

## Satellite Cloaking

### System Description

The concept of satellite cloaking takes stealth to a new level. To date, stealth has been a passive activity aimed at trying to minimize reflection and maximize absorption of energy with the goal of reducing the amount of energy reflected back to the sender. In contrast, cloaking will use active means to enable a satellite, as seen by enemy sensors, to blend into any environment.[28] Reliant on emerging material science advances as well as miniaturization and high-speed computing, a cloaked satellite will use nanotechnology robot films which will render it invisible in a space environment.

These nanotech materials, comprised of systems on the scale of individual molecules, must have two critical capabilities. First, the system must be capable of detecting any energy being aimed at the satellite. Is this possible? AT&T Bell Labs physicist Bernard Yurke sees nanotechnology systems with the sensitivity to "allow the first detection of individual photons."[29] After detection of incoming energy, the system must be capable of altering its construction to reflect or absorb that energy. With materials that have molecular motors and controllers, whole chunks of satellite skin can be made flexible and controllable. To simplify this idea of molecular manipulation, scientists describe nanotechnology through a vivid analogy. Picture an automated factory, full of conveyor belts, computers, and moving robot arms. Now imagine something like that factory but a million times smaller and working a million times faster with parts and pieces of molecular size.[30] In this concept the smart, adaptive skin of the spacecraft reacts to control inputs from the sensor array to make itself invisible to an enemy. In essence, molecular assembly lines are creating a satellite skin which is best suited to deflect or absorb incoming energy.

Figure 3-6 depicts a friendly satellite being radiated with radar energy from a hostile source. The sensor array on the surface of the friendly spacecraft detects inbound radar energy. The control system then directs the nanotechnology satellite skin to form a radar absorbent material and take an angular shape which will reflect the radar energy away from the source. Molecular sized computers, acting as the brains of this unique defensive shield, will enable the system to react almost instantaneously to inputs from the sensor array. The advent of nanocomputers, says Drexler, will give us practical machines with a trillion times the power of today's computers, all in a molecular package.[31]

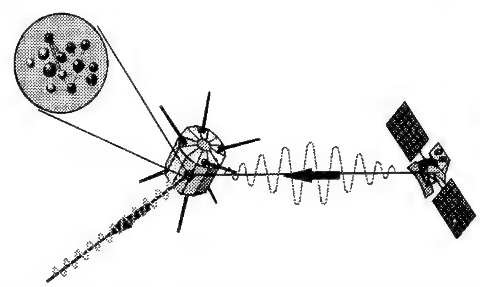


**Figure 3-6. Nanotechnology Cloaking System**

An alternate protective means is a stealthy satellite capable of generating an electrostatic or magnetic repulsion field which will shield the spacecraft from natural threats.[32] The repulsion field would be employed against low stress threats such as space debris or possibly to protect against solar flares. An important side benefit of such a repulsion field is the ability to use it as a sensor field to determine whether a satellite has been damaged by natural causes (space debris) or an attack. This capability gives the satellite controllers immediate information as to the probable cause should a satellite mysteriously drop off the screen.

Intelligent materials are another emerging technology with great possibilities in this

arena. Researchers are creating materials which, inspired by nature, can anticipate failure, repair themselves, and adapt to the environment. Smart materials employ tiny actuators and motors as muscles, sensors as nerves and memory, and computational networks that represent the brain and spinal column.[33] Molecular computers coupled with molecular sized assembly lines ready to build the right shield at the right moment with materials capable of adapting to the environment may make cloaking a reality in 2025.

As far as feasibility, Stewart Brand, a leading futurist at the Massachusetts Institute of Technology, reflects on nanotechnology, stating "the science is good, the engineering is feasible, the paths of approach are many, the consequences are revolutionary-times-revolutionary, and the schedule is: in our lifetimes."[34] Commercial interest in these technology developments, for uses in adaptive assembly lines and self-repairing machines, will increase the probability they will be available for incorporation in US space systems.

### Concept of Operations

The satellite cloaking system will operate on all space assets critical to US operations. This includes both military as well as key civilian spacecraft. The cloaking system will go into action once alerted by its onboard sensor array or warned by its command and control network.

First, the system will classify the incoming detection signal as radar, infrared, or visual (remember, individual photon detection is the norm). Sensor information is passed to the nanocomputer control system which relays commands to the nanobuilding blocks in the satellite skin. The building blocks, acting as their own molecular assembly lines, manufacture a skin which is optimized to reflect or absorb incoming energy. The ability to change at near instantaneous speeds allows the system to overcome the problem of suboptimal design (the trade-off between reflecting and absorbing materials) encountered in today's stealth aircraft. The nanotech spacecraft skin will be capable of battle damage repair to the spacecraft (a self-healing satellite). The ability to act autonomously to repair itself greatly reduces demand on the logistics system, which in space is a great advantage in both cost and time.

### Countermeasures

The most obvious countermeasure to a nanotechnology cloaking system is the ability to disrupt the molecular interactions which enable the system to operate. The possibility also exists for a new detection spectrum, possibly a smart beam, which is capable of changing to counter a response by the cloaking system. Destruction of smart nanotechnology materials should not pose a problem as the system will be capable of rejuvenation. However, this technology can be expected to proliferate through commercial developers to the community of space faring nations. The ability to perform the offensive counterspace mission against cloaked satellites presents its own unique challenges to US forces.

## Kinetic Energy Weapons

### General Discussion

Kinetic energy weapons (KEW) destroy things "the old-fashioned way," that is using energy generated by a moving mass impacting a target mass. KEW for space application in the form of antisatellite (ASAT) systems date back to the mid to late 1960s when both the US and Soviet Union were testing ASAT weapons. US commitment to an ASAT changed with administrations until testing was finally terminated in 1985 and the secretary of defense canceled the F-15 ASAT Program in 1988.[35]

KEW can be employed from the ground, air, or space against targets in any medium. This paper suggests concepts which employ KEW from various platforms against ground

and space targets. As noted previously, the space environment of the future will be one of multiple users of military, civil, and commercial satellites. In many cases, political considerations will prevent or severely constrain military options which involve actually destroying satellites. Having a solid KEW capability, however, will serve to deter similar aggression against US satellites and will give the US the option to destroy enemy satellites if necessary. Several concepts are proposed which take advantage of KEW technology. These include the satellite multiple attack and kill system (SMAKS) and Alpha Strikestar transatmospheric vehicle (TAV).

## Satellite Multiple Attack and Kill System

### System Description

This system (fig. 3-7) is similar to the Army's multiple launcher rocket system (MLRS), but instead of ground-to-ground capability the SMAKS employs a ground to space capability.[36] The system has three models designed for attacking low, medium, and high earth orbiting satellites. Similar to the Army system it is highly mobile and carries an array of antisatellite rockets. Given the potentially large number of enemy satellites existing in 2025, enough SMAKS vehicles are needed to ensure an effective ground-based ASAT capability over the entire battlespace. The system can also be based on ships and submarines to provide the capability of destroying launch vehicles in the boost phase before they can deploy enemy satellite systems. SMAKS carries highly sophisticated command and control, targeting, and positioning systems, requires minimum manning, and is readily deployable.

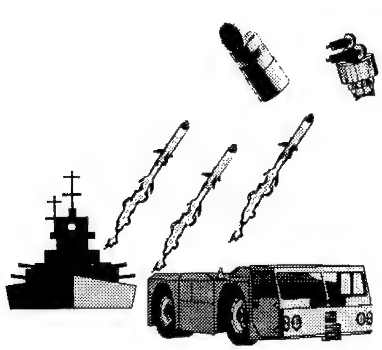


Figure 3-7. Satellite Multiple Attack and Kill System

### Concept of Operations

SMAKS is sized to fit easily into the air mobility workhorse of 2025 and must be located at appropriate locations depending on the target set. The system is sea-deployable giving it added flexibility. Using the advanced global positioning system (GPS), SMAKS will take a minimal amount of time to accurately locate itself and prepare itself to conduct antisatellite operations. Upon proper direction, the SMAKS will process appropriate targeting data received from surveillance and reconnaissance assets, upload the targeting data into the appropriate number of missiles, and release the weapons. Surveillance assets will conduct battle damage assessment and feedback to the SMAKS.

### Countermeasures

Potential countermeasures to this system would be electronic measures such as jamming and spoofing to confuse the required GPS information or other data links. Also while survivability is enhanced by using a mobile system, it is nevertheless vulnerable to attack from air or space while operating on the surface of the earth. Satellite maneuvering may be an effective countermeasure against a SMAKS type system that is heavily reliant on a target satellite's initial position and velocity for targeting.

## Alpha Strikestar Transatmospheric Vehicle

### System Description

The Alpha Strikestar is envisioned as a transatmospheric vehicle (TAV) able to take off and land horizontally and enter into low earth orbit.[37] (See fig. 3-8.) It is able to

transition between air and space environments repeatedly during the same mission, based on the threat and mission requirements. It carries multiple types of weapons to meet any threat. These include kinetic energy antisatellite missiles designed for total physical destruction and a high-powered laser cannon which is capable of disrupting, denying, degrading, or destroying unfriendly satellites. Another mission is the capture of an enemy satellite for return to earth or transfer to a useless orbit. The Alpha Strikestar is also air/space-to-ground capable using precision guided weapons to take out hard targets anywhere in the world on short notice. The vehicle is equipped with self-protective measures, as well as an imaging capability for battle damage assessment.

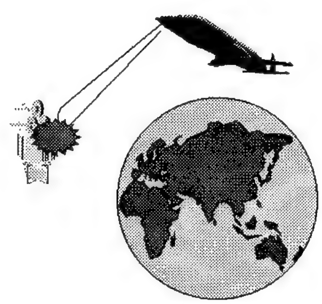


**Figure 3-8. Alpha Strikestar TAV**

### Concept of Operations

Alpha Strikestar can be scrambled to react to a crisis anywhere in the world on a moment's notice. Orbital insertion planning is preloaded into the weapons system computer to assist the pilot in proper positioning, target acquisition, and target engagement. For ground targets, mission planners will determine best application of weapons load (space or air delivered). The vehicle is flexible enough to enter low earth orbit en route to a ground target, reenter the atmosphere to deliver ordnance, then return to orbit to overfly the target and conduct battle damage assessment. If necessary the Alpha Strikestar can then reengage to complete the designated mission.

### Countermeasures

This system will employ state-of-the-art stealth technology, but if detected will be vulnerable to enemy ASAT attack, whether it be kinetic or directed energy. Since a TAV requires ground-based launch and processing facilities as well as runways, these are likely to be targeted as critical nodes by an enemy looking to ground a TAV fleet.

## Directed Energy Weapons

### General Discussion

Counterspace missions in 2025 will require the ability to disrupt, deny, degrade, and destroy enemy space capabilities. The proliferation of space users will reach monumental proportions in 2025, making counterspace attacks on individual users (the ground component) nearly impossible. The critical linkage between the user and the information he or she desires is the space-based asset and the transmitted data. Add to this situation the large future role of the space system entrepreneur and now attacking these systems may not only bring legal action against the US but may degrade our own capability. Directed Energy Weapons (DEW) of 2025 will provide the most promise for disrupting, degrading, denying, and if necessary destroying enemy space capabilities.

> A directed energy weapon must be able to generate energy, direct it on the target, propagate it through air or space, to the target, and induce some lethal effect in the target. Charged particle beams are probably the best at generating, directing, and killing but are clearly the worst at propagating. Neutral particle beams can propagate and kill but cannot yet be generated with sufficient intensities. Lasers are very good at directing and propagating, since light reflects from mirrors, can be pointed like a spotlight, and after leaving the weapon propagates in straight lines.[38]

Historically, the major drawback to DEW has been the necessity to operate in clear

weather. If the DEW is placed in space to conduct space-on-space attacks, this deficiency is eliminated. If the DEW is on the ground conducting earth-to-space attacks or in space conducting space-to-earth attacks, 2025 technologies for boring access holes through clouds and other obstructions may eliminate this deficiency. Development of a high-powered microwave weapon which can operate in all weather conditions may eliminate the poor weather deficiency. The current airborne laser (ABL), being developed to counter theater ballistic missiles, will demonstrate the ability of lasers to operate in environmental turbulence of the earth's atmosphere. The recently completed *New World Vistas Directed Energy Volume* report by the Air Force Scientific Advisory Board indicates, "the ABL will probably be the first practical and effective directed energy weapon to be deployed."[39] This will be the springboard to operating lasers through the medium of air and space. By 2025, DEW systems will likely operate in space and from the ground. This will give us the ability to negate objects in the atmosphere and in space. Five directed energy concepts were explored in this study.

## High Energy Laser Attack Station

### System Description

Disrupting, denying, degrading, and destroying enemy space capability will be accomplished by a space-based high-powered, short wavelength, solid state laser platform. This constellation of orbiting platforms will provide continuous, 24-hour protection of friendly forces and negation of enemy capabilities.[40] This constellation of counterspace platforms will be placed in low earth orbit (LEO—150 NM), medium earth orbit (MEO—11,000 NM), and geosynchronous orbit (GEO—22,000 NM). The high energy laser attack station (HELAS) will consist of 16 orbiting platforms at LEO, eight platforms at MEO, and four platforms at GEO. This multilevel constellation will provide a layered interactive defense against all space-borne or space-transiting threats. The multilevel system will protect all US assets in various altitudes and inclinations. A diode pumped solid state laser (DPSSL) will be the heart of the laser weapon subsystem. The DPSSL is more efficient than flashlamp pumping, which is the traditional method of exciting solid state lasers, and it results in much less heating of the laser as well.[41] Current solid state, chemical, and free electron lasers can generate power in the kilowatts range. However, a credible HELAS must employ lasers in the megawatt ranges. There appears to be no major technological limitation for DPSSL to achieve the megawatt range, and continued advancements will reduce the cost to reasonable limits.[42] (See fig. 3-9.)

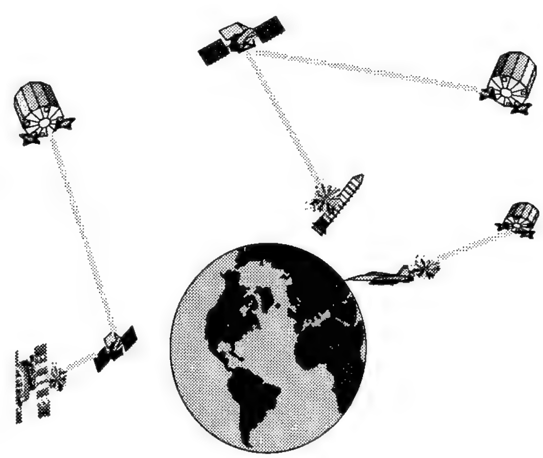


Figure 3-9. HELAS

### Concept of Operations

The HELAS will be the primary space attack/defense network for counterspace operations in 2025. The multilayer, multi-inclination constellation will be operated by a single ground crew member (ops chief) with the assistance of artificial intelligence health and maintenance software systems.[43]

Ground-based telemetry, tracking, and controlling will be conducted via satellite-to-satellite laser crosslinking. Another crew member will serve as the weapons manager who will track, target, and engage hostile targets. These two crew members can sit side by side in any size facility and in any location on the globe as long as they can communicate with at least one satellite. The crosslinking capabilities will provide the global command and control necessary to operate the constellation. Enemy ground launched or co-orbital ASAT can be detected, tracked, and engaged by HELAS. Although primarily a denial/destruction type weapon, the laser can be tuned to damage or degrade satellites by attacking subcomponents (i.e., solar array panels, reaction control thrusters, thermal heating of components to cause system shutdowns, etc.). Counterspace earth targets such as command and control ($C^2$) facilities, earth station antennas, spacelift facilities, and spacelift vehicles can also be effectively engaged by HELAS. The four GEO platforms could also provide dual-use capabilities for planetary defense by orienting HELAS outward. This could be done in a global emergency noting the degradation of the space defense mission with the GEO platform oriented outward.

### Countermeasures

Special reflective or absorbent material could make the laser ineffective. Use of low-observable or stealth technology may defeat targeting and identification systems on the HELAS. The HELAS may be vulnerable to antisatellite weapons or other laser stations. In addition, satellite hardening may be an effective countermeasure against low power laser pulses intended to degrade the target. This may force commanders to opt for the hard kill destruction of hardened satellites. A factor driving this decision will be the potential political impact of a turn in negative international opinion resulting from the total destruction of a satellite.

## Solar Energy Optical Weapon (SEOW)

### System Description

The SEOW will use the evolutionary concept of large orbiting structures to focus solar rays on earth and space targets to disrupt, deny, degrade, and destroy enemy capabilities.[44] This concept constructs a 10 kilometer magnifying glass or focusing element in space to illuminate targets on the ground or in space. This illumination can turn night to day on the ground, scorch facilities, or overheat satellite components. The solar energy provided to the focusing element on the weapon also provides a perpetual power source for the orbiting platform. Instead of using an orbiting magnifying glass to focus energy, another alternative is to use stored solar energy to power a directed energy weapon. A leap in battery technology leading to the capability to store immense quantities of power can be expected by 2025. (See fig. 3-10.)

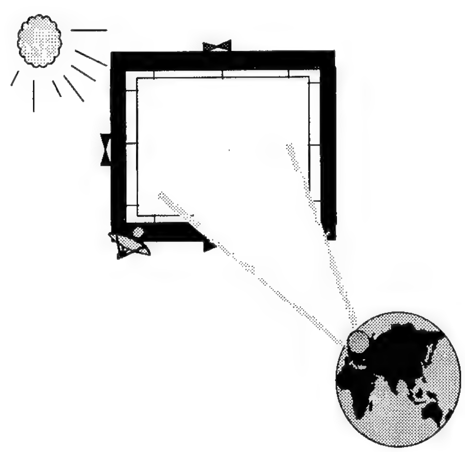


**Figure 3-10. Solar Energy Optical Weapon**

Large lightweight structures (kilometers) are feasible for 2025 and will provide the necessary stable platform to house the focusing or magnifying glass element. Advancements in space membrane structures and adaptive optics may provide the necessary capabilities to produce an

energy frugal space-based weapon. Each SEOW will orbit at geosynchronous altitude and consist of an Attitude Control System, Guidance, Navigation, and Control System, Reaction Control System, Targeting and Identification System, and the Laser Communications System.

**Concept of Operations**

The orbiting SEOW will be assembled in low earth orbit and boosted into geosynchronous orbit after the completion of the 10-kilometer optical focus assembly. The weapon can be maneuvered over the area of interest to provide space-to-earth capabilities as well. The solar energy can be spotted over a particular area of interest turning night into day. In addition, the beam could be focused on a power generation facility on the ground to provide a continuous high-energy source or the station could focus its beam on a lower orbiting satellite to provide it solar power when it would normally be in the earth's shadow. The beam could also be focused on an enemy orbiting threat to raise the internal temperature beyond functional limits. This may not destroy the satellite but, because of low sensitivity to heat, will force the automated shutdown of the satellite. Enemy controllers will only be able to detect the out-of-limit condition but will be unable to detect the source. For imaging and electronic surveillance satellites which pose a great threat to our forces (i.e., removes element of surprise), the SEOW will illuminate the target prior to its entry into the area of responsibility forcing an automated shutdown of the satellite or blinding of its sensors, thus preventing collection over our assets. Once the target has departed the protected area, illumination is discontinued until the next threat enters the area. Although this will completely deny use of the imaging/reconnaissance platform to all users for that period of time, US surveillance capabilities will be provided by other US government-controlled assets.

**Countermeasures**

As a large fragile target, the optic or space membrane could be easily disrupted or destroyed by KEWs or objects. Enemy forces could attempt to ram the weapon with a kamikaze satellite in hopes of rupturing the adaptive optic system. As a result, an active defense system will be needed to counter this potential threat. An alternative is to use a large number of small membranes coupled with adaptive optics to form a synthetic aperture type focusing element. This will make the array less vulnerable by dispersing the elements which make up the optics system.

## Electromagnetic Pulse (EMP) and High Power Microwave (HPM) Pills

**System Description**[45]

EMP radiation can be viewed as variations or created disturbances in the electromagnetic field which can cause disruption of electronic devices by arcing, overloading, and discharging. These EMP charges can be generated by numerous sources and can cause limited to extensive damage to electronic components. High power microwaves can penetrate external protective surfaces and disable or damage critical components of a satellite or other spacecraft. The HPM weapon might be focused on specific circuits and subcomponents within the target in order to disrupt or degrade mission functions.[46] Focusing and tuning the HPM to a specific wavelength or frequency might allow certain components to be isolated and affected. The EMP or HPM pills will be microsatellites which maneuver within close proximity of an enemy satellite and emit short-range pulses to interfere with the normal operation of the satellite.[47] These pills are intended for short duration operations in order to minimize the potential for collision with friendly satellites. These microsatellites will be launched into space by aircraft, transatmospheric vehicles (TAV), small launch

vehicles, or small fighter aircraft using high impulse air-to-space missiles. After 30 to 60 days, the pills will be directed to move to a collection orbit to be recaptured by TAV. The EMP/HPM pill will consist of small, lightweight satellites with an EMP gun or HPM generator attached. This compact, short-range weapon will provide an adequate offensive counterspace capability which will be undetected by the enemy. Because of the longer wavelengths and wider beams generated by EMP type weapons, pointing accuracy will not be as critical as those needed for laser type weapons. Although some EMP/HPM weapons exist today, the challenge for 2025 require miniaturization of the spacecraft and the applicable weapon (see fig. 3-11).

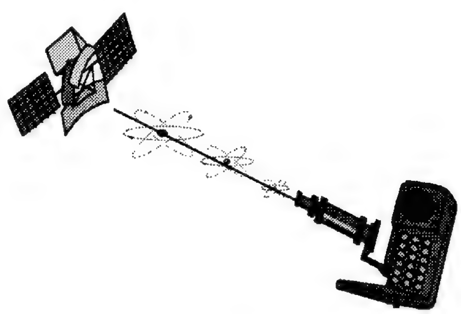


**Figure 3-11. EMP/HPM Pill**

### Concept of Operations

During prehostilities and during crises/war, EMP/HPM pills will be launched into orbit. These microsatellites will be positioned next to high-value enemy satellite systems and space systems operated by neutral countries or multinational corporations which may supply information to the enemy. The EMP/HPM pills will fly in formation with the enemy satellites until directed to engage. The explosive generator (or applicable weapon) will fire a fine tuned graduated pulse at the target. The goal is to deny the space capability through disruption and not destruction. This is especially true in the case of multinational corporation satellite systems. The pill can fire several rounds over a 60-day period at key times during the enemy satellite's orbit when it is collecting information on US forces or downlinking data to the ground. When the EMP/HPM pill has completed its mission or is no longer necessary, it can be deorbited and allowed to decay in the earth's atmosphere. The EMP/HPM pills can provide local neutralization of enemy satellite systems over the battlefield as well as global with a large number of cheap weapons.

### Countermeasures

System shielding and electrical ground may reduce the effectiveness of the EMP/HPM pill. If detected, the enemy could maneuver out of harm's way or fire a kinetic or directed energy weapon to degrade or destroy the EMP/HPM pill. Dispersion (spreading the mission over a larger number of smaller satellites) is another countermeasure. The resulting increase in numbers will force a corresponding increase in the number of EMP/HPM pills and will make degradation of the system more difficult. Our forces could counter by making EMP/HPM pills cheaper and easier to operate than the target satellite system.

## Ground-Based Laser (GBL)

### System Description

The GBL provides the capability to disrupt, deny, degrade, or destroy enemy space capabilities and potentially protect friendly space assets.[48] Several ground-based laser concepts have been explored over the past 25 years. Ground-based lasers offer unique advantages over space-based laser systems. Supportability and operability are major advantages to the ground-based laser. Deployment and supportability is functionally easier on a ground-based system than on an orbiting space system. There are two major drawbacks to ground-laser systems: line-of-sight limitations and atmospheric perturbation.

This concept will develop the laser station on the earth, fire the laser at relay optics in space, and use those relay mirrors to

engage targets either in space or on the earth. This places the most technically challenging component on the ground and deploys a very simple relay network system in orbit. Three to five laser generation sites will be placed in various locations across the continental United States (CONUS). These sites will have access to relay mirrors orbiting above, which can transfer the laser beam to other orbiting relay stations to attack targets on the other side of the globe. Dispersion of the laser stations and relay mirrors will help defeat the poor weather deficiency which has plagued the capability of ground lasers to fire through cloud cover into space. The Laser Guidestar program developed technology for atmospheric compensation which allows a ground telescope site to view a scene or irradiate a target anywhere around the globe while a relay mirror is in position to provide the view.[49] This technology will greatly contribute to our future ability to bounce lasers off orbiting mirrors to attack targets (fig. 3-12).

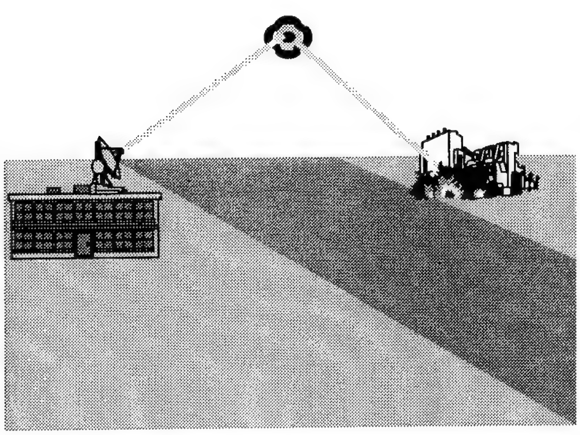


**Figure 3-12. Ground-Based Lasers**

## Concept of Operations

The five laser generation stations will be placed in those geographical locations best suited for laser operations and favorable weather conditions. Wide dispersion of these sites will increase the probability of having at least one site in clear weather for optimum operation. The laser generation site will be an unattended nuclear-powered facility which will provide the necessary megawattage required for the high-powered solid-state laser. Control of the five stations and the orbiting mirrors will be centralized in a primary facility with a mobile backup facility. Redundant satellite communications between the laser generation sites will increase survivability of the ground-based laser system. The orbiting mirrors will be laser crosslinked to reduce the ground support network for telemetry, tracking, and control (TT&C). The same reflecting mechanism used to attack a target can be used to identify and track the object before engagement. This information will be processed by ground computers at the central control facility and attack commands will be issued to the laser ground sites. Recycle times can be reduced to instantaneous rapid fire by using multiple laser generating sites to engage multiple targets. Different relay paths can be used to add redundancy to the system and also mitigate the problem of limited number of discharges by a single laser site.

## Countermeasures

Ground-based laser generation facilities are susceptible to conventional attack or sabotage. The orbiting mirrors will be susceptible to ASAT attack however, a large constellation of cheap orbiting mirrors is a natural counter to these measures. Excessively poor weather conditions across the entire CONUS will degrade the network capability. This may require overseas or outside the continental United States (OCONUS) basing (i.e., Hawaii, Alaska, Guam, Puerto Rico, etc.). The ability to actively modify weather conditions could be used to defeat a ground-based laser system by planting clouds over the laser site. On the other hand, the ability to remove cloud cover through weather modification may be an effective counter to

the effect of poor weather on ground-based lasers.

### Notes

1. *Technology Initiatives Game (TIG) 95* (Newport, R.I.: US Naval War College, 1995), 5-1.

2. Ibid., 147-1.

3. Ibid., 54.

4. Air University, *Air & Space in 2025 Research Study 2025*, Maxwell AFB, Ala., undated, counterspace team concept unnumbered. The space interdiction net is a possible technical approach to the problem of total battlespace awareness. Scientists argue that this may not be practical or possible by 2025. Taking this into account, this concept was rated low (i.e., beyond 2025) in the technology challenge area of the systems analysis.

5. John L. Peterson, *The Road to 2015* (Corte Madera, Calif.: Waite Group Press, 1994), 203.

6. Air University, *Air & Space in 2025 Research Study 2025*, Maxwell AFB, Ala., draft, excerpt from "Weather Modification, A Force Multiplier in 2025."

7. William Genoa, "Smallsats Come of Age," *Ad Astra*, November–December 1994, 2210.

8. Kaigham J. Gabriel, "Engineering Microscopic Machines," *Scientific American*, September 1995, 150.

9. USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century" (unpublished draft, the space technology volume, 15 December 1995), 49.

10. Robert Langreth, "Molecular Marvels," *Popular Science*, May 1993, 91.

11. "New World Vistas" (unpublished draft, the materials volume), 125.

12. ***2025*** Concept, no. 900432, "Mantle Communications System," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

13. K. Eric Drexler and Chris Peterson with Gayle Pergamit, *Unbounding the Future, The Nanotechnology Revolution* (New York: William Morrow and Company, Inc., 1991), 203.

14. Richard Szafranski and Martin C. Libicki, "'. . . Or Go Down in Flame?' Toward an Airpower Manifesto for the 21st Century," 4. Further information from Dr Libicki, INSS, Lecture to Air Command and Staff College, 25 March 1996.

15. Charles Babcock, "The Incredible Shrinking Computer," *Computerworld*, October 1993, 6.

16. Air University, *SPACECAST 2020–Volume II* (Maxwell AFB, Ala.; Air University Press, June 1994), M10–M13.

17. Air University, *SPACECAST 2020–Operational Analysis* (Maxwell AFB, Ala.; Air University Press, June 1994), 59–60.

18. ***2025*** Concept, no. 200049, "Satellite Reactive Armor (C007U)," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

19. ***2025*** Concept, no. 200170, "Electronic Signals Duplication," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

20. ***2025*** Concept, no. 900336, "Cloaking," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, no. 900338, "Stealth Technology," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, no. 900378, "Smart Metals Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996) and ***2025*** Concept, no. 900605, "Active Cloaking Film/'Paint'," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

21. Sun Tzu, *The Art of War* (Oxford: Oxford University Press, 1963), 66.

22. *Electronic Warfare Threat to US Communications* (U), Defense Intelligence Agency. (Secret) Information extracted is unclassified.

23. Ibid., 32.

24. Maj James G. Lee, *Counterspace Operations for Information Dominance* (Maxwell AFB, Ala.: Air University Press, 1995), 34.

25. Charles A. Fowler and Robert F. Nesbit, "Tactical Deception in Air-Land Warfare" (derived from Defense Science Board Study 1982–83), 17.

26. J. Jones, *Stealth Technology—The Art of Black Magic* (Blue Ridge Summit, Pa.: Tab Books, 1989), 2.

27. Ibid., 13.

28. ***2025*** Concept, no. 900336, "Cloaking," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, no. 900338, "Stealth Technology," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996); ***2025*** Concept, no. 900378, "Smart Metals Aircraft," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996) and ***2025*** Concept, no. 900605, "Active Cloaking Film/'Paint'," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996). Nanotechnology offers a very great return on investment if it can be applied to technologies such as cloaking or molecular-sized computers. This paper explores a possible technical approach to space stealth which some scientists argue will not be practical or possible by ***2025***. This concern is addressed in the systems analysis by assigning such systems a low score (i.e., probably beyond ***2025***) in the technology challenge category.

29. John Travis, "Building Bridges to the Nanoworld," *Science*, March 1994, 1703.

30. K. Eric Drexler and Chris Peterson with Gayle Pergamit, *Unbounding the Future, The Nanotechnology Revolution* (New York: William Morrow and Company, Inc., 1991), 20.

31. Ibid., 144–45.

32. ***2025*** Concept, no. 901178, "Space Debris Repulsion Field," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

33. Craig A. Rogers, "Intelligent Materials," *Scientific American*, September 1995, 154.

34. Ibid., 5.

35. Roger C. Hunter, *A United States Antisatellite Policy for a Multipolar World* (Maxwell AFB, Ala.: Air University Press, October 1995), 17–24.

36. Air University, *Air & Space in 2025 Research Study 2025*, Maxwell AFB, Ala., undated, counterspace team concept unnumbered.

37. ***2025*** Concept, no. 900292, "Alpha Strikestar Transatmospheric," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

38. Maj Steven R. Petersen, USAF, *Space Control and the Role of Antisatellite Weapons* (Maxwell AFB, Ala.: Air University Press, 1991), x.

39. "New World Vistas" (unpublished draft, the directed energy volume), vi.

40. ***2025*** Concept, no. 900420, "Laser Attack Station," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

41. "New World Vistas" (unpublished draft, the directed energy volume), x.

42. Ibid., vii.

43. Some scientists have argued the level of artificial intelligence required will not be achieved by ***2025***. This study acknowledges this debate, however, HELAS will gain most of its advantage from the ability to crosslink data and command throughout the entire constellation. This ability has just been demonstrated with the current Milstar constellation. The ability to use artificial intelligence for routine satellite "state of health" will be the next milestone, preceded by the ability to handle all TT&C responsibilities.

44. ***2025*** Concept, no. 900163, "Solar Energy Weapon," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

45. ***2025*** Concept, no. 900270, "EMP Pills," ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

46. E. E. Cassagrande, *Non-lethal Weapons: Implications for the RAAF* (Fairbain, Australia: Air Power Studies Centre, 1995), 4.

47. The EMP/HPM pill is a possible technical approach to solving the problem of clandestine attack on a space adversary's system. An energy source sufficient to fire EMP or HPM bursts as well as a propulsion system to maneuver the pill into position are technology areas which must be addressed. Some scientists have argued that these technology advances will not be practical or possible by ***2025***.

48. "New World Vistas" (unpublished draft, the directed energy volume), vi.

49. Ibid.

## Chapter 4

# Concept of Operations for a Counterspace Architecture

To assure US space superiority over the global battlespace, all elements of the enemy's space infrastructure and system of systems must be put at risk. Counterspace operations can be offensive or defensive and future commanders will require a variety of counterspace tools to engage various threat scenarios. Offensive counterspace operations seek to neutralize enemy space capabilities before they can be employed against friendly forces. Offensive counterspace missions will target enemy space capabilities on the ground (such as ground control stations or space launch complexes), assets already in space, and satellite communication links.[1] To protect our vast array of high leveraged satellite systems, defensive counterspace will neutralize hostile threats. Defensive counterspace systems will protect both military and civilian space assets and deny any enemy the ability to degrade the effectiveness of US space systems. Both offensive and defensive space missions are required to fully achieve space superiority.

## Offensive Counterspace Operations

Within our offensive counterspace architecture, several previously discussed concepts will provide the means to deny, degrade, disrupt, and, if necessary, destroy enemy space capabilities. To identify and monitor space up and down link communications, the Space Interdiction Net concept will provide instantaneous monitoring and accurate identification of any space communication to or from the ground via space-based systems. Unique links may be targeted for denial, disruption, degradation, or destruction while preserving friendly signal integrity. The Space Interdiction Net provides commanders complete space situational awareness as well as a number of discrete options to target enemy links. This is very important considering multinational use of identical space systems when only one nation may be the offensive counterspace target. The Space Interdiction Net concept provides this valuable service, with or without knowledge of the space system's owning country or corporation. Blended with space targeting and detecting systems (laser designators, anti-ASAT subsystems, and gravity gradiometers), offensive space systems will target the entire spectrum of enemy space capabilities. Soft kill systems such as robo-bugs and EMP/HPM pills will selectively jam or interrupt a satellite's signals without destroying it. Jamming the data transmission from the sensor to the ground user will not be sufficient in 2025. Once the sensor has collected the data (in the case of surveillance and reconnaissance), the data can be dumped to suitcase size receivers any where on the globe. Instead of targeting the data stream, it may be necessary to halt the collect of the information. EMP/HPM pills, robo-bugs, and other soft-kill or temporary blinding weapons will prevent collection over the area or interest which stops the mission at the input stage. This capability greatly increases flexible response options available to space battlefield commanders (see fig. 4-1).

At the more resolved end of the counterspace spectrum lies physical destruction of enemy space capabilities. Force-on-force engagements may be necessary to destroy enemy capabilities or resupply efforts. Directed energy weapons (ground- or space-based lasers, Strikestar TAV) provide commanders instantaneous destruction options for global and theater control. Kinetic energy weapon systems (surface, air, or space based), because of range and time limitation may

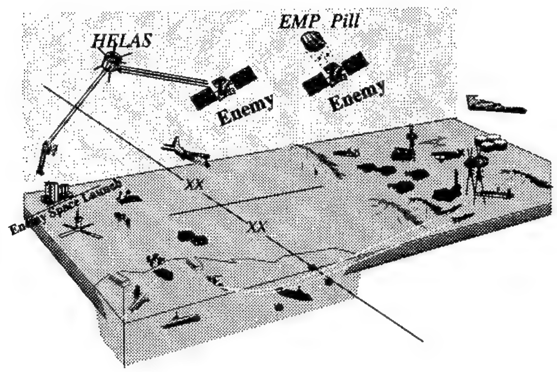



**Figure 4-1. Offensive Counterspace Architecture**

best provide kill capabilities in the area of responsibility however, they can also engage globally from prepositioned locations. With a variety of offensive counterspace weapons to provide flexible engagements options to decision makers, we must also possess responsive and capable defensive counter-space systems.

## Defensive Counterspace Operations

Defensive counterspace operations consist of active and passive measures designed to reduce the effectiveness of enemy space systems targeted against friendly interests. Active defense measures detect, identify, intercept, and disrupt or destroy threatening space systems. Passive defense involves protecting friendly space assets by satellite design and maneuver, warning commanders of enemy space threats, and minimizing these threats though camouflage, emission control, deception, and decoys, thus denying the enemy space data.[2] The Space Interdiction Net provides a valuable defensive capability by monitoring, and if necessary, targeting enemy communication links. In addition, capabilities such as cloaking and satellite bodyguards will be integrated to protect friendly space assets. Successfully employing coordinated offensive and defensive counterspace operations leads to space superiority. The High Energy Laser Attack Station (HELAS) and Ground Based Laser (GBL) offer immediate defensive kill capability. These flexible defensive systems can provide near instantaneous response to detected and identified threats to our space system (fig. 4-2).

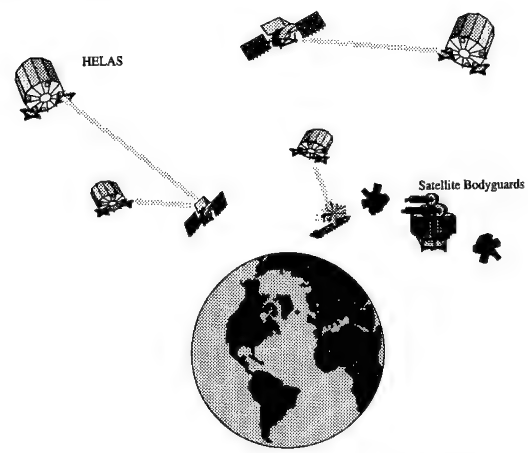



**Figure 4-2. Defensive Counterspace Operations**

As more and more nations expand commercially and militarily into space, space superiority will make the difference between victory and defeat in future wars. Many nations learned a great deal from the Persian Gulf War. They noted not only the significance of precision-guided munitions but also the importance of space-based force enhancement.[3] Space is the ultimate high ground—a center of gravity in any future conflict. Whoever commands that high ground in all forms will dominate future warfare.

### Notes

1. Air Force Doctrine Document 4, "Space Operations Doctrine" (first draft), 15 August 1995, 12–13.
2. Ibid., 13.
3. Lt Col Michael R. Mantz, *The New Sword: A Theory of Space Combat Power* (Maxwell AFB, Ala.: Air University Press, 1995), 6.

# Chapter 5

# Investigation Recommendations

Space has been called the final frontier, the ultimate high ground, and the wave of the future. Space systems have long been recognized for their contributions to the national security of the US and have proven themselves invaluable in the conduct of modern warfare. As we approach the battlefield of 2025, we must recognize that because space is so totally integrated into the fight, we have no choice but to protect friendly space assets through defensive and offensive counterspace operations as necessary to prevent an adversary from exploiting space systems against the US. Today, we stand on the threshold of an era which will see massive integration of space systems into the way of life of the nations of the world. Those that most effectively leverage space systems will be the political, economic, and military leaders of the world of 2025.

In order to make sure the US stays out in front in space power, we must begin planning now for the counterspace architecture of 2025. Key to this effort is to be proactive in developing the technologies, systems, and operational concepts for counterspace, rather than waiting until an adversary threatens, or worse, destroys one or more US space assets. This paper has discussed key technology areas required to implement certain promising concepts to achieve space superiority. These technologies are detection and targeting, miniaturization, stealth, kinetic energy weapons, and directed energy weapons.

Detection and targeting is a key technology area which is critical to the effective employment of counterspace weapons. Dominant battlespace awareness is critical in achieving space superiority. This area is especially challenging in the 2025 space environment where satellites are used by commercial and military users alike and we must have the capability to identify and target only the appropriate parts of a mission payload or its signal. Next, miniaturization must be pursued to reduce the critical aspects of size, weight, and cost when lifting large numbers of satellites into orbit. Work going on now in the areas of microelectromechanical systems, microtechnology and nanotechnology must continue and be tested in order to determine space applications. Given the likely threat capabilities of potential adversaries in 2025, the next technology, stealth, is especially critical to passively and inexpensively protecting US satellites from attack. This type of stealth is the application of nanotechnology and molecular manipulation to make satellites invisible to sensors. There is significant research, development, and testing going on in this area, and it must continue. A fourth area, kinetic energy weapons, will provide the needed capability to hold enemy satellites at risk of total destruction. This capability has already been proven from the air. Technology advances are needed to make this a capability from the ground in large numbers. Finally, the most promising means of force application lie in the area of directed energy weapons. Today the airborne laser is well on its way to operational status. This system must continue to be supported so that it can prove the feasibility of laser weapons. The follow-on efforts to airborne laser will need to prove directed energy weapons can be operated from air to space and within space. An analysis aimed at prioritizing these concepts with recommendations for future development follows.

## Future Concepts—A System Analysis

In order to determine which of the counterspace concepts presented in this paper are most likely to yield the maximum return on

investment, we have attempted to rank them using a subjective system analysis. Each system is scored in a number of categories which represent those characteristics most likely to contribute to air and space superiority in 2025. In addition, the systems have been scored in areas representing cost, schedule, and technical feasibility (table 3). The categories used to score the systems are

**Commercial Applicability** - The extent to which the concept has technology spin-offs which contribute to the commercial sector. (5 = very high commercial application; 1 = very low commercial application).

**Availability** - Probability that the system will be operational in 2025. (5 = very probable; 1 = very improbable).

**Payback** - Return on investment will be very critical, especially in a world in which the defense budget is shrinking. (5 = very high return on investment; 1 = very low return on investment).

**Contribution to Air and Space Superiority** - Probability that a particular system will spur a military technical revolution in 2025 (a silver bullet system). (5 = revolutionary contribution to air and space superiority; 1 = minimal contribution).

**Cost** - An order of magnitude estimate of system cost. (5 = system cost measured in millions; 3 = system cost measured in billions; 1 = system cost measured in trillions).

**Lethality** - Probability of kill (for offensive systems) or probability to prevent hard kill (for defensive systems). (5 = very high probability of kill/save; 1 = very low probability of kill/save).

**Selectivity** - Represents the range of options a system offers in terms of offensive or defensive capabilities. For offensive systems, selectivity measures the ability to inflict hard kill, soft kill, or both. For defensive systems, selectivity represents the ability to protect against hard kill, soft kill, or both. (5 = offers all options [hard kill, soft kill, both]; 1 = offers no options).

**Technology Challenge** - The probability that technology will advance enough in key areas to provide the capability described in the concept. (5 = forecast by 2025; 4 = plausible by 2025; 3 = possible by 2025; 2 = beyond 2025; 1 = well beyond 2025).

Based on this subjective analysis of the counterspace systems developed in this paper, a natural break in the scores appears. Those systems which fall "above the line (score of 30 or better), would seem to offer the greatest potential to contribute significantly to control of the air and space environment in 2025. Those systems (in priority order according to table 3 and table 4) are

1. Space Interdiction Net (32)
2. Alpha Strikestar TAV (32)
3. Robo-bugs (32)
4. EMP/HPM Pills (31)
5. Ground Based Laser (30)
6. Satellite Bodyguards (30)

In ranking the concepts at the top of the list, a number of factors were considered. Developing the Space Interdiction Net by 2025 pushes the technology development envelope to its maximum. However, the return is a silver bullet system which could significantly impact the way any future war in space is waged. On the other hand, the Alpha Strikestar TAV and robo-bugs offer exceptional capabilities but do not make the revolutionary impact on how war is waged that the Space Interdiction Net offers (table 4).

Each of the systems presented will rely heavily on breakthroughs in miniaturization and high-speed computing, both technologies which should see significant commercial development in the future. It is critical that the military capitalize on these advances in technology to develop systems that will offer uncontested access and control of space. Investment in systems such as those presented here will provide this capability in the future. The challenge is to move from the present to the future—where Star Tek is used to exploit the final frontier.

**Table 3**

**System Analysis Score Sheet: Miniaturization, Stealth, and Detection/Targeting Concepts**

| | SATELLITE BODYGUARDS | ROBO-BUGS | SATELLITE CLOAKING | SMAKS | GRAVITY GRADIOMETER | ANTI-ASAT | SPACE INTERDICTION NET |
|---|---|---|---|---|---|---|---|
| Commercial Applicability | 2 | 2 | 4 | 2 | 2 | 1 | 4 |
| Availability | 4 | 4 | 2 | 4 | 3 | 3 | 3 |
| Payback | 4 | 5 | 3 | 3 | 3 | 2 | 5 |
| Contribution to Air/Space Superiority | 4 | 5 | 3 | 3 | 2 | 3 | 5 |
| Cost | 3 | 4 | 2 | 3 | 3 | 3 | 2 |
| Lethality | 5 | 4 | 4 | 3 | 3 | 3 | 5 |
| Selectivity | 4 | 5 | 3 | 2 | 3 | 3 | 5 |
| Tech Challenge | 4 | 3 | 2 | 5 | 2 | 4 | 3 |
| Total | **30** | **32** | **23** | **25** | **21** | **22** | **32** |

**Table 4**

**System Analysis Score Sheet: Kinetic Energy and Directed Energy Concepts**

| | ALPHA STRIKESTAR TAV | HIGH ENERGY LASER ATTACK STATION | SOLAR ENERGY OPTICAL WEAPON | EMP/HPM PILLS | GROUND BASED LASER |
|---|---|---|---|---|---|
| Commercial Applicability | 4 | 2 | 4 | 4 | 2 |
| Availability | 4 | 3 | 2 | 4 | 4 |
| Payback | 5 | 4 | 4 | 3 | 4 |
| Contribution to Air/Space Superiority | 5 | 5 | 4 | 4 | 4 |
| Cost | 2 | 1 | 2 | 5 | 3 |
| Lethality | 4 | 5 | 4 | 4 | 5 |
| Selectivity | 4 | 3 | 4 | 4 | 3 |
| Tech Challenge | 4 | 4 | 3 | 3 | 5 |
| Total | **32** | **27** | **27** | **31** | **30** |

# Appendix A

# Evolving Space Doctrine in the '90s

## Space Superiority as an Air Force Core Competency

In 1994 the secretary of the Air Force set three goals for the Air Force in space. The first of these goals was to make space support to the war fighter routine. Air Force Space Command has made significant progress toward this goal and continues its intensive effort to provide timely, effective space support to war fighters commanding and executing conventional campaigns. As we rapidly move toward routine space operations for war-fighting support, the need to establish and maintain freedom of operations in space becomes increasingly critical. In a speech to the Air Force Historical Foundation in the fall of 1995, Secretary Sheila E. Widnall stated, "Space superiority has emerged as a critical element of today's military operations. Support from space is becoming the quintessential force multiplier."[1] Indeed space superiority is one of five core competencies illuminated in the secretary of the Air Force and AF chief of staff's recent Air Force Executive Guidance (fig. A-1). Core competencies are fundamental contributions provided by the Air Force for national security.

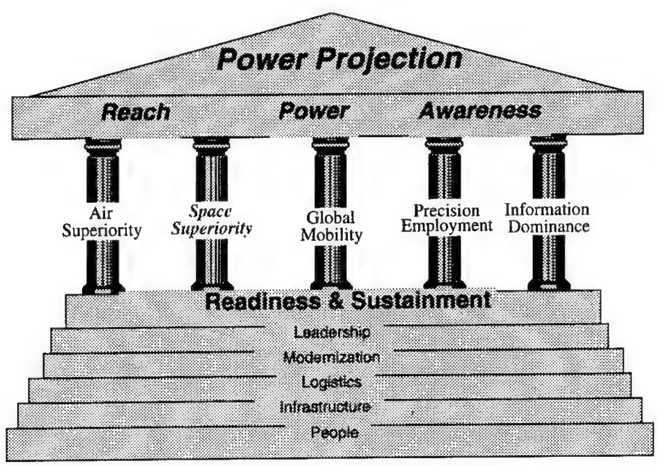



**Figure A-1. Core Competencies**

These core competencies are founded on readiness and sustainment, and they support global reach, global power, and global awareness as air and space forces project power around the globe.[2] Space superiority as a core competency derives from deep historical roots dating to the 1950s in which the Air Force has led the way in space. Today, as the leaders in space, the USAF controls 80 percent of the Department of Defense (DOD) space budget and incorporates 90 percent of DOD's space personnel. The Air Force supports this core competency with an annual budget of $5 billion.[3] USAF space assets make a real and substantial contribution to US national security.

Space superiority involves a sufficient degree of control to ensure US and allied forces freedom of position, maneuver, employment, and engagement in space, and it involves the ability to deny this freedom to adversaries. To date the US has not had to fight to gain and maintain space superiority. This will change as the US becomes increasingly reliant on space forces to fight and win its wars, and as the use of space systems proliferates to more and more nations around the world. In recognition of this, the Air Force Executive Guidance states the following assumption and guidance, "Air and Space superiority will continue to be an essential element of US war-fighting capability (as well as) fielding relevant, capable space forces is a modernization priority that spans the near-, mid-, and long-term."[4] In its discussion of Air Force core competencies, the draft Air Force Doctrine Document 1 (AFDD 1) equates space superiority to air superiority in terms of critical importance, and it recognizes that control of space may actually secure freedom of operations in all geographical environments.[5] Having explored space superiority as one of the five Air Force core competencies, it is now important to take a look at the evolving Air Force doctrine for this critical area.

## Evolving Space Superiority Doctrine

Space superiority is achieved through counterspace operations. The current Air Force Manual 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 2, March 1992, provides a limited treatment of counterspace under "Aerospace Control Missions." The document categorizes offensive counterspace operations as those conducted against an enemy's systems which operate in space, and defensive counterspace as missions to defend against attacks by systems operating in space. The key discriminator in differentiating between counterair missions and counterspace missions is the location of the target. If the target resides in space then the mission is counterspace regardless of the medium from which the force is applied. If the target resides in the atmosphere, then the mission is counterair.[6] New and evolving doctrine gives more thorough treatment to the space medium.

The new draft Air Force Doctrine Document 1, "Air Force Basic Doctrine," lays out space superiority as one of the Air Force's five core competencies. This new document along with a new draft Air Force Doctrine Document 4, "Space Operations Doctrine," provides a more extensive treatment of those aspects of space forces which support control of space. Space control assures a level of freedom of friendly use of space while denying this freedom to the enemy. Counterspace controls activities both in and through the space environment. An important aspect to understand is counterspace operations may be conducted by air, land, sea, special operations, as well as space forces. Like counterair it includes both offensive and defensive aspects.[7]

Offensive counterspace operations can be of a lethal or nonlethal nature as they disrupt, deny, degrade, or destroy the enemy's space systems or the information they provide. Disruption is considered to be the temporary impairment of the use of space systems and normally does not involve physical damage. Jamming is a good example of disruption. Denial refers to the temporary elimination of the use of space systems but still does not normally involve actual physical damage. An example of denial would be cutting off power to critical ground nodes. Degradation takes things a step further by permanent impairment of the use of space systems, normally through physical damage. Attacks against ground nodes would be an

example of this. Finally, destruction is physical damage which permanently eliminates the utility of the space system. Use of airpower to bomb a space uplink or downlink facility falls into this category. Offensive counterspace actions are taken at a time and place of our choosing and can include attacks from space- or terrestrial-based forces on any or all segments of the enemy's space systems to include space vehicles, ground stations, and the signals emanating from both.[8]

Defensive counterspace preserves the ability to operate freely in and through space by reducing or precluding the effectiveness of the adversary's counterspace capabilities. There are two types of defensive counterspace operations, active and passive. These are defined below.

> The objective of active defense is to detect, track, identify, intercept, and destroy or neutralize enemy space and missile forces. Active defense operations include maneuvering the satellite, deploying mobile ground links and terrestrial elements, and deploying decoys.
>
> The objectives of passive defense are to reduce the vulnerabilities and to protect and increase the survivability of friendly space forces and the information they provide. Passive defense includes measures such as encryption, frequency hopping, and hardening.[9]

The new draft doctrine also identifies two important contributing capabilities to the counterspace mission: surveillance and reconnaissance of space and ballistic missile warning. Surveillance and reconnaissance of space provide the situational awareness and targeting which are essential to conducting effective counterspace operations. In addition, both space-based and ground-based systems perform detection, tracking, and reporting of ballistic missile events. These functions are critical to determining potential ballistic missile threats to the North American land mass, US operations worldwide, as well as space systems.[10]

The preceding discussion of current and evolving doctrine is intended to provide a departure point for discussing counterspace operations in 2025. To circumscribe the remaining discussion, we must look to where the Air Force leadership wants us to go in the relative near-term as we then leap to 2025. The Air Force Executive Guidance document provides vectors across all areas of core competency including relevant assumptions and specific guidance statements. These assumptions and associated guidance are of such importance that they are quoted here from the Executive Guidance:

## Offensive Counterspace

**Assumptions:**

1. US reliance on space-based capabilities will continue to increase.

2. The number of national and nonnational entities utilizing space-based assets to gain advantage will increase.

3. Space situational awareness is critical to space control.

**Guidance:**

1. The Air Force will continue to improve its ability to disrupt, deny, degrade, or destroy adversary space assets or capabilities.

2. The Air Force must survey space and protect its ability to use space while preventing adversaries from interfering with that use.

## Defensive Counterspace

**Assumptions:**

1. Protection, denial, and negation capabilities are core and essential to space control.

2. The Air Force must expect and be prepared to defend against attacks (physical or electronic) on our space systems and facilities.

3. Protecting and assuring US access to space systems employment is essential to protecting US vital interests.

4. Protection of national security space systems capabilities using traditional measures such as deception, ground/space segment hardening, and secure $C^4I$ techniques and nontraditional measures through integration of defensive Information Warfare measures are necessary to achieve adversary uncertainty about US intentions, plans, and operations.

5. Protecting the Earth and our space-based assets against damage from extraterrestrial objects deserves consideration.

**Guidance:**

1. The Air Force must continue to enhance its denial, protection and negation capabilities.[11]

Although fairly general in nature, the three guidance statements above give us a leaping off point to imagine the road down which the Air Force must travel to achieve a truly robust counterspace capability in the year 2025. One last data point for framing the challenge of future counterspace operations is to understand what counterspace capabilities the Air Force employs today.

## How the Air Force Does Counterspace Today

Today our counterspace capabilities are limited and primarily defensive and passive in nature. To the extent possible, US military satellite systems are hardened against electromagnetic pulse and radiation. Currently, secure command, control, and communications techniques (frequency hopping, low probability of intercept/low probability of detection, and signal encryption) are employed. Communications crosslinking provides added survivability against ground station attacks and robust system employment. Satellite subsystems are designed and built with double and triple redundancy. Large satellite constellations such as the global positioning system are dispersed to allow for graceful degradation should a small number of satellites be lost from the constellation. In addition, satellites carry fuel on board for station keeping operations which, given sufficient warning, could be used for maneuvering to attempt to avoid attack. Clearly these measures fall into the defensive counterspace realm whereby we are trying to reduce the vulnerabilities and increase the survivability of friendly space forces and the information they provide.

Perhaps the greatest amount of infrastructure and effort in defensive counterspace today lies in the extensive battle management and command, control, and communications (BM/$C^3$) capability of the Space Defense Operations Center (SPADOC) at Cheyenne Mountain Air Force Base, Colorado. The SPADOC is responsible for defense of US and allied space systems through monitoring and reporting on unusual space activity and planning possible defensive countermeasures. It assesses possible threat attack information and determines

which friendly systems are vulnerable. The SPADOC is a data fusion center with wide connectivity to all space systems owners and operators through the Space Defense Command and Control System.[12] In a hostile space environment such as that expected in 2025, today's simple countermeasure will not be sufficient to protect US space systems and critical nodes such as SPADOC will be vulnerable.

**Notes**

1. The Honorable (Dr) Sheila E. Widnall, secretary of the Air Force, "Space: No Longer a Secret," address to the Air Force Historical Foundation, Washington, D.C., 21 September 1995.

2. *Air Force Executive Guidance*, December 1996, 5–6.

3. Widnall.

4. *Air Force Executive Guidance*, 7–8.

5. Air Force Doctrine Document 1, "Air Force Basic Doctrine" (first draft), 15 August 1995, 9.

6. Air Force Manual 1-1, *Basic Aerospace Doctrine of the United States Air Force*, vol. 2, March 1992, 104–5.

7. Air Force Doctrine Document 4, "Space Operations Doctrine" (proposed final draft), 8 November 1995, 4.

8. Ibid., 4–5.

9. Ibid., 5.

10. Ibid.

11. *Air Force Executive Guidance*, 9.

12. AU-18, *Space Handbook*, vol. 1, *A Warfighter's Guide to Space* (Maxwell AFB, Ala.: Air University Press, 1993), 103.

# Bibliography

***2025*** Concept, no. 200049, "Satellite Reactive Armor (C007U)." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 200170, "Electronic Signals Duplication." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900163, "Solar Energy Weapon." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900270, "EMP Pills." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900292, "Alpha Strikestar Transatmospheric." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900336, "Cloaking." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900338, "Stealth Technology." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900378, "Smart Metals Aircraft." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900420, "Laser Attack Station." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900432, "Mantle Communications System." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 900605, "Active Cloaking Film/'Paint'." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

***2025*** Concept, no. 901178, "Space Debris Repulsion Field." ***2025*** concepts database (Maxwell AFB, Ala.: Air War College/***2025***, 1996).

Air Force Doctrine Document 4. "Space Operations Doctrine" (first draft), 15 August 1995.

Air University. *SPACECAST 2020–Volume II*. Maxwell AFB, Ala.: Air University Press, June 1994.

______. *SPACECAST 2020–Operational Analysis*. Maxwell AFB, Ala.: Air University Press, June 1994.

AU-18, *Space Handbook. A Warfighter's Guide to Space*. Vol. 1. Maxwell AFB, Ala.: Air University Press, 1993.

Asker, James R. "Space Control." *Aviation Week & Space Technology*, 23 May 1994, 57.

Babcock, Charles. "The Incredible Shrinking Computer." *Computerworld*, October 1993, 6.

Barnett, Jeffery R. *Future War, An Assessment of Aerospace Campaigns in 2010*. Maxwell AFB, Ala.: Air University Press, 1996.

Cassagrande, E. E. *Non-lethal Weapons: Implications for the RAAF*. Fairbain, Australia: Air Power Studies Centre, 1995.

Defense Intelligence Agency. *Electronic Warfare Threat to US Communications* (U). (Secret) Information extracted is unclassified.

Drexler, K. Eric, and Chris Peterson with Gayle Pergamit. *Unbounding the Future, The Nanotechnology Revolution*. New York: William Morrow and Company, Inc., 1991.

Fowler, Charles A., and Robert F. Nesbit. "Tactical Deception in Air-Land Warfare." Derived from Defense Science Board Study 1982–83.

Gabriel, Kaigham J. "Engineering Microscopic Machines." *Scientific American,* September 1995, 150.

Genoa, William. "Smallsats Come of Age." *Ad Astra,* November–December 1994, 2210.

Hunter, Roger C. *A United States Antisatellite Policy for a Multipolar World.* Maxwell AFB, Ala.: Air University Press, October 1995.

Johnson, Nicholas L. *Soviet Military Strategy in Space.* New York: W. W. Norton & Co., 1986, 155.

Joint Warfighting Center Doctrine Division. "Warfighting Vision 2010" (draft). Fort Monroe, Va., 1995.

Jones, J. *Stealth Technology—The Art of Black Magic.* Blue Ridge Summit, Pa.: Tab Books, 1989.

Langreth, Robert. "Molecular Marvels." *Popular Science,* May 1993.

Lee, Maj James G. *Counterspace Operations for Information Dominance.* Maxwell AFB, Ala.: Air University Press, 1995.

Libicki, Dr Martin C., and Col Richard Szafranski. "'. . . Or Go Down in Flame?' Toward an Airpower Manifesto for the 21st Century," 1996.

Mantz, Lt Col Michael R. *The New Sword: A Theory of Space Combat Power.* Maxwell AFB, Ala.: Air University Press, 1995.

Petersen, Maj Steven R. *Space Control and the Role of Antisatellite Weapons.* Maxwell AFB, Ala.: Air University Press, 1991.

Peterson, John L. *The Road to 2015.* Corte Madera, Calif.: Waite Group Press, 1994.

Piotrowski, Gen John L. "A Soviet Space Strategy." *Strategic Review,* Fall 1987.

Prepared Statements of Gen Charles Horner, commander in chief, United States Space Command, in Senate. *Space Seen as Challenge, Military's Final Frontier* (Defense Issues, Prepared Statement to Hearings before the Senate Armed Services Committee, 90th Cong., 1st sess., 1993, 7).

Radabaugh, Capt Gregory C. "Soviet Antisatellite Capabilities." *Signal,* December 1988, 81–83.

Rogers, Craig A. "Intelligent Materials." *Scientific American,* September 1995, 154.

Schneider, Barry R. "Battlefield of the Future." In *The Revolution in Military Affairs.* Maxwell AFB, Ala.: Air University Press, 1995.

Travis, John. "Building Bridges to the Nanoworld." *Science,* March 1994, 1703.

Tzu, Sun. *The Art of War.* Oxford: Oxford University Press, 1963.

USAF Scientific Advisory Board. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft, the Directed Energy Volume. 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft. Space Applications Volume, 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft. Space Technology Volume, 15 December 1995.

_____. "New World Vistas: Air and Space Power for the 21st Century." Unpublished draft. Materials Volume, 15 December 1995.

US Naval War College (USNWC). *Technology Initiatives Game (TIG) 95,* Newport, R.I., 1995.

**APPENDIX A**
**Index of *2025* Volumes**

## Books

*Executive Summary*

*Alternate Futures for **2025**: Security Planning to Avoid Surprise*

*An Operational Analysis for **2025**: An Application of Value-Focused Thinking to Future Air and Space Capabilities*

## White Papers

### Volume 1: Awareness

"Information Operations: Wisdom Warfare for 2025"

"Worldwide Information Control System (WICS)"

"2025 In-Time Information Integration System ($I^3S$)"

"The Command or Control Dilemma: When Technology and Organizational Orientation Collide"

"Joint Readiness Assessment and Planning Integrated Decision System (JRAPIDS): Combat Readiness and Joint Force Management for 2025"

"Virtual Integrated Planning and Execution Resource System (VIPERS): The High Ground of 2025"

"The Man in the Chair: Cornerstone of Global Battlespace Dominance"

"Brilliant Warrior"

"Brilliant Force and the Expert Architecture That Supports It"

"Brilliant Warrior: Information Technology Integration in Education and Training"

### Volume 2: Reach and Presence

"Logistics in 2025: *Consider It Done!*"

"Dynamic Response Logistics: Changing Environments, Technologies, and Processes"

"2025 Aerospace Replenishment: The Insidious Force Multiplier"

"Airlift 2025: The First with the Most"

"Spacelift 2025: The Supporting Pillar for Space Superiority"

"Spacenet: On-Orbit Support in 2025"

"Procurement in 2025: Smarter Ways to Modernize"

"Aerospace Sanctuary in 2025: Shrinking the Bull's-Eye"

**Volume 3, Book 1: Power and Influence**

"Frontier Missions: Peacespace Dominance"

"Information Operations: A New War-Fighting Capability"

"Information Attack: Information Warfare in 2025"

"A Contrarian View of Strategic Aerospace Warfare"

"Interdiction: Shaping Things to Come"

"Hit 'em Where It Hurts: Strategic Attack in 2025"

"Close Air Support (CAS) in 2025: 'Computer, Lead's in Hot' "

"Counterair: The Cutting Edge"

"Star Tek—Exploiting the Final Frontier: Counterspace Operations in 2025"

**Volume 3, Book 2: Power and Influence**

"Surfing the First and Second Waves in 2025: A Special Operations Forces Strategy for Regional Engagement"

"The DIM MAK Response of Special Operations Forces to the World of 2025: Zero Tolerance/Zero Error"

"A Hypersonic Attack Platform: The $S^3$ Concept"

"Strikestar 2025"

"Space Operations: Through the Looking GLASS (Global Area Strike System)"

"Weather as a Force Multiplier: Owning the Weather in 2025"

"Planetary Defense: Catastrophic Health Insurance for Planet Earth"

**Volume 4: Special Studies**

"Paths to Extinction: The US Air Force in 2025"

" ' . . . Or Go Down in Flame?' An Airpower Manifesto for the Twenty-First Century"

"An Operational Analysis for 2025: An Application of Value-Focused Thinking to Future Air and Space Capabilities" (technical report)

**Volume 5: Information Warfare** (Classified)

"Knowledge Warfare: Shattering the Information War Paradigm"

"INCAPACATTACK: The Strings of the Puppet Master"

"C-Net Attack"

# APPENDIX B
# Project Participants

## AIR UNIVERSITY

**Lt Gen Jay W. Kelley**
Commander
Air University
***2025*** Study Chair

**Col Richard Szafranski**
***2025*** Study Director

**Col Joseph A. Engelbrecht, Jr.** (F)
***2025*** Research Director

**Col Michael D. Kozak**
***2025*** Support Director

## AIR WAR COLLEGE

### FACULTY

Col Larry D. Autry (A)
Col Miles A. Baldwin (A)
Col Victor P. Budura (A)
Col Richard R. Crawford (USMC)
Col Theodore C. Hailes IV (A)
Col Tamzy J. House (A)
Lt Col Thomas P. Brehm (A)
Lt Col Stefan Eisen, Jr. (A)
Lt Col Thomas Mahr (USA) (A)
Capt Gene A. Smith (USN)
Dr David C. Blair (A)
Dr Richard L. DiNardo
Dr Judith A. Gentleman (A)
Dr Grant T. Hammond (A)
Dr James A. Mowbray (A)
Dr Irene Pearson-Morrow (A)
Dr Mark R. Shulman (A)
Dr David S. Sorenson (A)
Dr George J. Stein (A)
Mr Michael L. McKim (A)
Mr Stephen I. Schwab (A)

### STUDENTS

Col Henry D. Baird (T)
Col Marvin S. Mayes (T)
Col Charles B. Oltman (T)
Col (Sel) John M. Andrew (O, T)
Col (Sel) Robert L. Atkins, Jr. (T)
Col (Sel) Bruce W. Carmichael (T)
Capt Clarence E. Carter (USN) (T)
Col (Sel) James A. Cerniglia (USA) (T)
Col (Sel) Rick W. Lester (T)
Col (Sel) Yoshio Smith (T)
Col (Sel) John M. Urias (USA) (T)
Lt Col David Atzhorn (T)
Lt Col Thomas F. Baldy (T)
Lt Col Thomas F. Berardinelli (T)
Lt Col Robert L. Bivins (F, G, T)
Lt Col William W. Bradley, Jr. (T)
Lt Col James A. Fellows (T)
Lt Col Robert D. Gaudette (T)

A = faculty advisor; E = Executive Committee Group briefer; F = Alternate Futures Development Team member; G = White Paper Development Group leader; O = Operations Analysis Team member; T = White Paper Development Team leader

Comdr Steven M. Jacobsmeyer (USN)
Lt Col Duane A. Lamb (G)
Lt Col Norman K. Leonpacher (T)
Lt Col Gregory J. Miller (E, G, T)
Lt Col Michael M. Miller
Lt Col Dawn M. Moll (E, G)
Lt Col Alphronzo Moseley (T)
Lt Col Edward F. Murphy (T)
Lt Col William B. Osborne (USA) (T)
Lt Col Steven W. Rapp (T)
Lt Col Gregory A. Roman (E, G)
Lt Col Duane R. Schattle (USMC)
Lt Col William B. Shields (USA) (T)
Lt Col Carol S. Sikes (T)
Lt Col David M. Snyder (T)
Comdr Suzanne K. Spangler (USN) (G)
Lt Col Jeffrey E. Thieret (T)
Comdr Ronald J. Unterreiner (USN) (T)
Lt Col Jamie G. G. Varni (T)
Lt Col Robert M. Worley II
Lt Col Robert H. Zielinski (T)
Ms Marlene L. Barger (G)
Ms Judy L. Edgell (T)
Mr Gregory M. Powers

### ADDITIONAL CONTRIBUTORS

Ms Iole M. De Angelis

## AIR COMMAND AND STAFF COLLEGE

### FACULTY

Col Ronald A. Winter
Lt Col Deborah Beatty
Comdr Homer J. Coffman (USN)
Lt Col Thomas Mahoney
Lt Col James B. Near, Jr.
Lt Col Patrick D. Nutz
Lt Col Kermit Phelps
Maj Phillip A. Chansler
Maj Neil Couch
Maj Michael R. Foster
Maj Robert S. Gordon
Maj Ed F. Greer
Maj Anthony L. Hardin
Maj Doug Johnston
Maj George E. Spencer III
Maj Eduardo L. Vargas
Maj James F. Wooddell
Dr Glen L. Spivey

### STUDENTS

Maj Steven D. Acenbrak (USA)
Maj Larry N. Adair
Maj Donald A. Ahern
Maj John M. Aiken
Maj Gary C. Bender
Maj Scott A. Bethel
Maj Jim C. Bigham, Jr.
Maj Sandra R. Bignell
Maj Douglas S. Black
Maj Carl H. Block
Maj Christopher W. Bowman
Maj Jeff A. Brelsford
Maj Joseph T. Callahan III
Maj David B. Carr
Maj John R. Carter, Jr.
Maj Jack S. Caszatt
Maj Ronald J. Celentano
Maj Richard M. Chavez
Maj Nolen R. Chew
Maj Louise A. Christ
Maj Patrick M. Condray (F)
Maj Harry W. Conley (O)
Maj Christopher A. Cook
Maj Dan S. Crawford
Maj William T. Davidson, Jr.
Maj Steven J. DePalmer
Maj Troy E. Devine
Maj Teresa L. Dicks
Maj Penny J. Dieryck
Maj Laura A. H. DiSilverio
Maj Gregory F. Dragoo
Maj William E. Durall

Maj Deborah Y. Eves
Maj Kurt C. Fecht
Maj Merrily D. Fecteau (F)
Maj George W. Fenimore III
Maj Richard J. Findlay (USMC)
Maj Terrence J. Foley
Maj Lisa A. Friend
Maj Linda K. Fronczak
Maj John P. Geis II (F)
Maj Edward M. Griffin
Maj Ronald A. Grundman
Maj Frederick I. Guendal, Jr.
Maj William J. Harding
Maj Michael R. Hargrove
Lt Comdr Michael H. Harner (USN)
Maj Stephen G. Harris
Lt Comdr Mark J. Hellstern (USN)
Maj Scott A. Henderson
Maj Kyle K. Holmquist
Maj John F. Hunnell
Maj David M. Husband
Maj Michael J. Irwin
Maj Leonard W. Jackson
Maj Barbara Jefts
Maj Kevin R. Joeckel
Maj David C. Johnson
Maj Craig E. Jordan
Maj Gregory J. Juday
Maj Bruce M. Juselis
Maj Robert J. Kaufman
Maj Kelvin P. Kearney
Maj Steven S. Kempf
Maj Douglas L. Kendall
Maj Kevin G. Kersh
Maj Wesley W. Long
Maj Kent S. Lund
Lt Comdr Ernest B. Markham (USN)
Maj Edwin L. Marsalis, Jr.
Maj James M. Maxwell
Maj Samuel J. McCraw
Maj Ann E. Mercer
Maj Thomas K. Moore
Maj Cynthia L. A. Norman
Maj Philip M. Nostrand
Maj Theodore P. Ogren
Maj Matthew A. Parks
Maj Patrick E. Pence
Maj Thomas G. Philipkosky
Maj Jennifer L. Pickett
Maj Curtis O. Piontkowsky
Maj Patrick A. Pope
Maj James E. Pugh
Lt Comdr Alfredo E. Rackauskas (USN)
Maj Joseph M. Roeder
Maj Michael C. Ruff
Maj Laura J. Sampsel (USMC)
Maj Claire M. Saucier
Maj Larry J. Schaefer
Maj Michael M. Shepard
Maj Michael A. Silver
Maj Philip S. Simonsen
Maj Kevin C. Smith (F)
Maj Patrick J. Smith
Maj Stephen M. Tanous
Maj Michael J. Tiernan
Maj Kenneth R. Tingman
Maj Michael F. Wagner
Maj Mark E. Ware
Maj Michael F. Welch
Maj YuLin G. Whitehead
Maj Richard S. Wilcox
Maj Charles W. Williamson III
Maj Timothy M. Zadalis
Maj Felix A. Zambetti III
Maj David W. Ziegler
Lt Ronald Reis (USN)
Dr Adelaide K. Cherry
Mr James L. Pullara
Mr Michael J. Wadzinski

## EXECUTIVE COMMITTEE

**Lt Gen Ralph E. Eberhardt, Chairman**
Deputy Chief of Staff
Plans and Operations
United States Air Force

**Lt Gen Patrick P. Caruana**
Vice-Commander
Air Force Space Command

**Lt Gen Brett M. Dula**
Vice-Commander
Air Combat Command

**Lt Gen John C. Griffith**
Vice-Commander
Air Education and Training Command

**Lt Gen Jay W. Kelley, Study Chair**
Commander
Air University

**Lt Gen Everett H. Pratt, Jr.**
Vice-Commander
United States Air Forces Europe

**Lt Gen Charles T. Robertson, Jr.**
Vice-Commander
Air Mobility Command

**Lt Gen Eugene D. Santarelli**
Vice-Commander
Pacific Air Forces

**Lt Gen Thad A. Wolfe**
Vice-Commander
Air Combat Command

**Maj Gen Lawrence P. Farrell, Jr.**
Vice-Commander
Air Force Materiel Command

**Maj Gen Robert A. McIntosh**
Vice-Commander
Air Force Reserve

**Maj Gen Donald W. Shepperd**
Director
Air National Guard

**Brig Gen James L. Higham**
Vice-Commander
Air Force Special Operations Command

**Brig Gen Howard J. Ingersoll**
Vice-Commander
Air Force Special Operations Command

## ADVISORY GROUP

**Dr Anthony K. Hyder, Chairman**
Associate Vice President for Graduate Studies
Professor of Aerospace Engineering
University of Notre Dame

**Gen Michael P. C. Carns, USAF, Retired**
Managing Partner
Pyle Carns Initiatives

**Adm Bobby Inman, USN, Retired**
Consultant

**Gen Robert W. RisCassi, USMC, Retired**
Vice President
Land Systems
Loral Corporation

**Gen Bernard A. Schriever, USAF, Retired**
Consultant

**Vice Adm William E. Ramsey, USN, Retired**
Vice President
Corporate Business Division
CTA Incorporated

**Maj Gen Joe H. Engle, ANG, Retired**
Deputy for Independent Review Team
Shuttle *Mir*

**The Honorable Emory Folmar**
Mayor
City of Montgomery, Alabama

**Dr Alf Andreassen**
Managing Partner
Industry Planning
AT&T Solutions

**Dr Norman R. Augustine**
President
Lockheed Martin Corporation

**Dr Daniel Hastings**
Associate Department Head for Research
Professor of Aeronautics and Astronautics
Massachusetts Institute of Technology

**Dr Richard H. Kohn**
Chairman of Curriculum in Peace, War, and Defense
University of North Carolina, Chapel Hill

**Dr Gene H. McCall**
Chairman, USAF Scientific Advisory Board
Laboratory Fellow
Los Alamos National Laboratory

**Mr James Cameron**
Hollywood Director and Screenwriter
Light Storm Entertainment

**Ms Natalie W. Crawford**
Associate Director
Project Air Force
RAND

**Mr Frederick D. Gregory**
Associate Administrator
Office of Safety and Mission Assurance
National Aeronautics and Space Administration

**Mr Burt Rutan**
Chief Executive Officer
Scaled Composites, Inc.

**Mr Dag M. Syrrist**
Vice President
Environment Finance Group
Technology Funding

## AIR FORCE INSTITUTE OF TECHNOLOGY

**Col Gerald A. Hasen, Team Chief** (O)
Lt Col Karen W. Currie (T, W)
Lt Col Gregg H. Gunsch (O, T)
Lt Col Jack A. Jackson (O, W)
Lt Col Brian L. Jones (O, T)
Lt Col Stuart C. Kramer (T, W)
Maj Thomas A. Buter (O, T)
Maj Lee J. Lehmkuhl (O, W)
Maj Robert F. Mills (O)
Maj Terrance L. Pohlen
Capt Gerald F. Ashby
Capt Darren J. Buck
Capt Christopher Burke
Capt James A. From
Capt Scott R. Maethner
Capt Edward A. Pohl
1st Lt Robert W. Carneal IV
1st Lt Brian I. Robinson
1st Lt Gregory E. Wood
Dr Craig M. Brandt
Dr Christopher D. Hall
Dr Alan R. Heminger
Dr D. Kirk Vaughan
Ms Janet E. Hill (T)
Ms Sally F. Tirone (T)

## SUPPORT STAFF

Col Michael D. Kozak, Director
Lt Col Howard P. Funkhouser, USAF, Retired, Deputy Director
Lt Col Dan A. Novak, Deputy Director
Lt Col Larry L. Boyer
Capt Arthur E. Rice
Capt John E. Vice II
Capt Stacey L. Waldrep
TSgt Ronald E. Franks
SSgt Brian S. Sommers

O = Operations Analysis Team member; T = Technology Team member; W = White Paper Development Team leader

SrA Laura A. Wiggins
Mr Russell S. Mathews
Ms Mary L. McCann
Ms Bridgit A. Pena
Mr Joe L. Roberts
Ms Deborah H. Smith

## COLLEGE OF AEROSPACE DOCTRINE, RESEARCH, AND EDUCATION

Lt Col John L. Furr
Maj John R. Reese
Capt Jeffrey J. Closson
Capt Eddie C. Harris
MSgt John M. Seeley

## RESEARCH COORDINATOR'S OFFICE

**Col Charles G. White, Director**
Lt Col Thomas S. Kelso
Capt Stacey L. Waldrep
TSgt Jimmy J. Wills
SSgt Lynn Blankenship

## UNITED STATES AIR FORCE ACADEMY

Maj Earl McKinney (T)
Dr John Bertin (T)
Cadet John M. Boehm
Cadet Matt Bruhn
Cadet Scott Dyer
Cadet Greg Ellingson
Cadet Iain D. M. Ferguson
Cadet Jed Hutchinson
Cadet Stephen B. Matthews
Cadet Josh McClure
Cadet Tom McElhinney
Cadet Thomas C. McIntyre
Cadet Brandon L. Rasmussen
Cadet Adam R. Sitler
Cadet J. Brett Taylor
Cadet Robert A. Williamson
Cadet George R. Wyse

## AIR UNIVERSITY PRESS

### EDITORIAL SUPPORT

Ms Emily Adams
Dr Richard Bailey
Ms Debbie Banker
Ms Lula Barnes
Dr Marvin Bassett
Mr Preston Bryant
Ms Susan Carr
Ms Joan Hickey
Mr John Jordan
Mr Tom Mackin
Ms Carolyn McCormack
Ms Hattie Minter
Dr Glenn Morton
Ms Pat Richards
Ms Peggy Smith
Ms Bessie Varner

T = White Paper Development Team leader

**GRAPHICS SUPPORT**

Mr Daniel Armstrong
Ms Linda Colson
Ms Susan Fair
Mr Steve Garst
Ms Becky McLeod

**PUBLICATIONS SUPPORT**

Ms Mary Ferguson
Mr Tom Lobenstein

## AIR UNIVERSITY TELEVISION

**Maj Dale G. Derr, Director**
SrA Klinton Kraft
Mr Charles Caton
Mr Ray Dobbs
Mr Warren Jones, Jr.

## GUEST SPEAKERS

**Gen Ronald R. Fogleman**

Chief of Staff
United States Air Force

**Adm William A. Owens (USN)**

Vice-Chairman
Joint Chiefs of Staff

**Lt Gen Jay W. Kelley**

Commander
Air University

**Lt Gen Anthony C. Zinni (USMC)**

Commanding General
1st Marine Expeditionary Forces

**Maj Gen John P. Casciano**

Director, Joint Command and Control Warfare Center
Commander, Air Intelligence Agency

**Maj Gen I. B. Holley, Jr., USAFR, Retired**

Department of History
Duke University

**Maj Gen John R. Landry, USA, Retired**

National Intelligence Officer for General Purpose Forces
Central Intelligence Agency

**Maj Gen Charles D. Link**

Special Assistant for Roles and Missions
Office of the Chief of Staff
Headquarters USAF

**Rear Adm Richard A. Wilson (USN)**

Deputy Director
Space and Electronic Warfare
OPMAV

**Brig Gen Orest L. Kohut**

Deputy Director
Eighth Quadrennial Review of Military Compensation

**Col Joseph A. Engelbrecht, Jr.**

***2025*** Research Director
Air War College Deputy Chairman
Department of Conflict and Change

**Col Mike S. Francis**

Program Manager
Advanced Research Project Agency

**Col Tom L. Harkins (USMC)**

Commandant's War-Fighting Laboratory
Marine Corps Combat Development Command

**Col Gerald A. Hasen**
***2025*** Technology Team Leader
Air Force Institute of Technology

**Col William G. Heckathorn**
Director
Advanced Weapons and Survivability Directorate
Phillips Laboratory

**Capt William D. Henry (USN)**
Director of Information Warfare
National Security Agency

**Col Michael D. Kozak**
***2025*** Support Director
Air War College

**Col Paul E. Morton**
Research Physician
Armstrong Laboratory

**Col Thomas F. Page**
Commander
Headquarters US Army Training and Doctrine Command

**Col Chet Richards, Jr. (USAFR)**
Business Strategist
Lean Enterprise
Lockheed Aeronautical Systems Company

**Col Michael D. Starry (USA)**
Director
Future Battle Directorate
Headquarters US Army Training and Doctrine Command

**Col Richard Szafranski**
***2025*** Study Director
Air War College National Military Strategy Chair

**Col John A. Warden III, USAF, Retired**
President and CEO
Venturist, Inc.

**Col Charles G. White, Jr.**
Chairman
Research Coordinator's Office
Air War College

**Col Simon P. Worden**
Commander
50th Space Wing
Falcon AFB, Colorado

**Lt Col Denny Ehrler**
Deputy Director for Analysis Support
National Reconnaissance Office

**Lt Col Martin N. Fracker**
Chief
Research Operations Office
Armstrong Laboratory

**Lt Col Gregg H. Gunsch**
***2025*** Technology Team Member
Air Force Institute of Technology

**Lt Col Thomas S. Kelso**
Deputy Director
Research Coordinator's Office
Research Plans and Policy
Air Command and Staff College

**Lt Col Jack N. Summe**
Directorate of Plans, Policy, and Strategic Assessments
USSOCOM/SOJ5

**Maj Lee J. Lehmkuhl**
***2025*** Technology Team Member
Air Force Institute of Technology

**Dr John L. Anderson**
Manager
Technology Frontiers Studies
NASA Headquarters

**Dr Oleg Y. Atkov**
Cosmonaut
Cardiologist

**Dr Arnold A. Barnes, Jr.**
Senior Scientist
Atmospheric Sciences Division
Phillips Laboratory

**Dr Paul J. Berenson**
Scientific Advisor to Commander
Headquarters US Army Training and Doctrine Command

**Dr Peter Bishop**
Associate Professor of Human Sciences
Chair of Graduate Programs and Studies of Futures
University of Houston, Clear Lake

**Dr Peter F. Bytherow**
Applied Physics Laboratory
The Johns Hopkins University

**Dr Wladimiro Calarese**
Chief Scientist
Air Force Institute of Technology

**Dr Gregory H. Canavan**
Senior Scientist
Los Alamos National Laboratory

**Dr Martin van Creveld**
Author and Professor
Hebrew University, Jerusalem

**Dr Stephen E. Cross**
Director
Information Technology Center
Carnegie Mellon University

**Dr John Dasoulous**
Applied Physics Laboratory
The Johns Hopkins University

**Dr Grant T. Hammond**
Department of Core Electives
Air War College

**Dr Charles B. Hogge**
Chief Scientist
Lasers and Imaging Directorate
Phillips Laboratory

**Dr Robert L. Jeanne**
Entomologist
University of Wisconsin

**Dr Gilbert G. Kuperman**
Mathematician-Technical Director
Crew Station Integration Branch
Armstrong Laboratory

**Dr James T. Kvach**
Chief Scientist
Armed Forces Medical Intelligence Center

**Dr Martin Libicki**
Senior Fellow
National Defense University

**Dr Armin K. Ludwig**
Department of Conflict and Change
Air War College

**Dr Gene McCall**
Chairman, Scientific Advisory Board
Laboratory Fellow, Los Alamos National Laboratory

**Dr Dennis Meadows**
Director
Institute for Policy and Social Science Research
University of New Hampshire

**Dr Gregory S. Parnell**
Assistant Professor of Mathematical Sciences
Virginia Commonwealth University

**Dr Stephen Rogers**
Professor of Electrical Engineering
Air Force Institute of Technology

**Dr George J. Stein**
Chairman
Department of Conflict and Change
Air War College

**Dr Gary J. Sycalik**
Vice President
Innovative Futures

**Dr Alvin Toffler**
Author, *Future Shock* and *The Third Wave*
Futurist

**Dr Eli Zimet**
Head of Special Programs Department
Office of Naval Research

**Mr Bill Arkin**
Writer and Consultant
Greenpeace

**Mr Garry Barringer**
Director
Plans and Programs Directorate
Rome Laboratory

**Mr James A. Bowden**
Senior Analyst
Scientific Applications International Corporation

**Mr Carl H. Builder**
Senior Member, Researcher
RAND

**Mr Jeffrey R. Cooper**
Senior Researcher
Science Applications International Corporation

**Mr Robert G. Dodd**
Operations Analyst
Headquarters US Army Training and Doctrine Command

**Ms Ellen R. Domb**
Instructor/Facilitator
PQR Group
Goal Quality-Productivity-Competitiveness

**Ms Anne DuFresne**
Office of Weapons, Technology, and Proliferation
Chemical and Biological Warfare Branch
Central Intelligence Agency

**Mr Fritz Ermarth**
Senior Central Intelligence Agency Officer
Office of the Director of Central Intelligence

**Mr Kaigham J. Gabriel**
Deputy Director
Electronics Technology Office
Advanced Research Project Agency

**Mr Glen Gaffney**
Chief
Information Warfare Branch
Office of Scientific and Weapons Research
Central Intelligence Agency

**Mr Joe Haldemann**
Author and Professor
Massachusetts Institute of Technology

**Mr Walt Hazlett**
Chief
Liaison and Planning Section
Central Intelligence Agency

**Mr Robert H. Justman**
Producer
Late Harvest Productions

**Mr Kevin Kelly**
Author and Editor
*Wired* Magazine

**Mr Robert King**
Executive Director
Goal Quality-Productivity-Competitiveness

**Ms Christine A. R. MacNulty**
President
Applied Futures, Inc.

**Ms Janice M. Marconi**
Creatologist-Creativity: Innovation Research Team
Goal Quality-Productivity-Competitiveness

**Mr Andy Marshall**
Director
Net Assessments
Office of the Secretary of Defense

**Mr Edward Neumeier**
Hollywood Screenwriter
*Robocop*

**Mr Darrell Spreen**
Directed Energy Panel Ad Hoc Advisor
Phillips Laboratory

## STUDY CONSULTANTS

**Gen Larry D. Welch, USAF, Retired**
President and CEO
Institute for Defense Analysis

**Maj Earl McKinney**
Tenured Associate Professor
US Air Force Academy

**Dr James J. Wirtz**
Assistant Professor of National Security
Naval Postgraduate School

**Mr John Marrs**
Program Manager
National Information Display Laboratory

**Mr Terry L. Neighbor**
Chief of Investment Strategy
Wright Laboratory

**Mr Chip Pickett**
Director
Analysis Center
Northrop-Grumman Corporation

**Mr Charles M. Sheppard, Jr.**
Air Force Representative
UAV Joint Technology Steering Committee
Wright Laboratory

## ASSESSORS (Visiting)

**Brig Gen Charles Stebbins**
Vice President and Manager
R&D Operations
LOGICON RDA

**Col Mike Francis**
Program Manager
Advanced Research Project Agency

**Col George Haritos**
Deputy Director and Commander
Air Force Office of Scientific Research
Air Force Institute of Technology

**Col Paul Morton**
Research Physician
Armstrong Laboratory

**Col Thomas F. Page**
Commander
Headquarters US Army Training and Doctrine Command

**Col Michael L. Smith**
Director
Joint Doctrine Directorate
Headquarters US Army Training and Doctrine Command

**Col Richard Ward II**
Director
Plans, Programs, and Resources
Headquarters Space Warfare Center

**Lt Col David Curdy**
Chief
Concept Division
Headquarters Space Warfare Center

**Lt Col William Rember**
Chief
Staff Operations Group
Pentagon

**Maj Paul C. Gibbons**
Action Officer
$C^4I$ Systems
Marine Corps Combat Development Command

**Maj Michael B. Leahy, Jr.**
Technical Investment Manager
Wright-Patterson AFB, Ohio

**Maj Ed O'Connell**
Chief
Commander's Action Group
Headquarters Air Intelligence Agency

**Maj Gregg Sparks**
Chief
Air-to-Surface IPT
Wright-Patterson AFB, Ohio

**Maj Rich Stephenson**
Transport and Aerial Delivery Concepts Manager
Headquarters Air Combat Command

**CMSgt Vic Tidball**
Superintendent of the Future Concepts Division
Plans and Analysis Directorate
Air Force Command, Control, Communications, and Computer Agency

**Dr Wade Adams**
Chief Scientist
Materials Directorate
Wright Laboratory

**Dr Paul J. Berenson**
Scientific Advisor to the Commander
Headquarters US Army Training and Doctrine Command

**Dr John Bertin**
Professor
Department of Aeronautics
US Air Force Academy

**Dr Charles Bridgman**
Associate Dean for Research
School of Engineering
Air Force Institute of Technology

**Dr Dennis M. Bushnell**
Chief Scientist
National Aeronautics and Space Administration
Langley Research Center

**Dr Wladimiro Calarese**
Chief Scientist
Air Force Institute of Technology

**Dr Robert L. Crane**
Materials Research Engineer
Wright Laboratory

**Dr Dan DeLaurentis**
Aerospace Systems Design Laboratory
Georgia Institute of Technology

**Dr David Gorney**
Director
Research and Development
The Aerospace Corporation

**Dr John T. Hanley**
Deputy Director and Program Coordinator
Naval War College

**Dr Paul Herman**
Senior Analyst
Office of National Security Issues
Defense Intelligence Agency

**Dr Charles B. Hogge**
Chief Scientist
Lasers and Imaging Directorate
Phillips Laboratory

**Dr Thomas W. Hussey**

Chief
High Energy Sources Division
Kirtland AFB, New Mexico

**Dr Sam Lambert**

Chief Scientist
Armament Directorate
Wright Laboratory

**Dr William S. Lummas**

Chief Scientist
National Military Intelligence Production Center

**Dr Dimitri Mavris**

Aerospace Systems Design Laboratory
Georgia Institute of Technology

**Dr Paul McManamon**

Acting Associate Chief Scientist of the Avionics Directorate
Wright Laboratory

**Dr David Moorhouse**

Acting Chief Scientist
Flight Dynamics Directorate
Wright Laboratory

**Mr William F. Ballhaus, Jr.**

Vice President
Science and Engineering
Lockheed Martin Corporation

**Mr Kenneth Becker**

Chief of Automated Information Systems Branch
Air Force Command, Control, Communications, and Computer Agency

**Mr Dennis L. Carter, PE**

Senior Aerospace Engineer
Wright Laboratory

**Mr Octavio Diaz**

Manager
Program Support
Operations Analysis Staff
Boeing Defense and Space Group

**Mr Paul Hashfield**

Program Manager
National Information Display Laboratory

**Mr Howard D. Irick**

General Engineer
US Army Space and Strategic Defense Command

**Mr Robert T. Kohout**

Army Research Laboratory Liaison Officer
Headquarters US Army Training and Doctrine Command

**Ms Christine A. R. MacNulty**

President
Applied Futures, Inc.

**Mr Dick Mueller**

Senior Specialist
Program Development
McDonnell Douglas Aerospace Corporation

**Mr Darrell Spreen**

Technical Advisor
Phillips Laboratory

**Mr Dale von Hasse**

Director of Aerospace Science
Lockheed Martin Corporation

## ASSESSORS (Internet)

**Col Thomas J. Berry**

HQ AMC/CCX

**Col Edward Leonard**

Hickam AFB, Hawaii

**Lt Col Peter M. Bailey**
HQ AMC/XPDS

**Lt Col Michael L. Crawford**
PL/WS

**Lt Col Frank E. Dressell**
HQ AMC/XPDL

**Lt Col David A. Honey**
HQ ESC/XRT

**Lt Col Michael H. Taint**
HQ AFMC/XPP

**Lt Col Joseph E. Toole**
ESC/TG-4

**Maj Howard R. Blakeslee**
SMC/XRT

**Maj Thomas N. Contos**
HQ AMC/XPDSC

**Maj Ronnie E. Edge**
938 EIS/ISU

**Maj M. Clarke Englund**
HQ USAF/SCT

**Maj Daniel C. Favorite**
HQ AMC/XPDSC

**Maj Stephen C. Hallin**
HQ ESC/XRC

**Maj Keith A. Michel**
HQ AMC/XPDSP

**Maj John Peterson**
HQ AFSOC/XPXS

**Maj Ronald F. Richard**
HQ AFSOC/LPP

**Maj Jeffrey S. Woolston**
ACC/SCXP

**Capt Matthew B. Ash**
HQ AFSOC/XPPD

**Capt William D. Briton**
OO-ALC/LIW

**Capt Thomas E. Deeter**
SA-AI/TIES

**Capt James G. Holden**
SMC/XRT

**Capt Michael E. Santos**
AEDC/XPR

**Dr Robert J. Bunker**
Claremont, California

**Dr Joseph C. Foster, Jr.**
Eglin AFB, Florida

**Dr David Gorney**
The Aerospace Corporation

**Dr Rhonald M. Jenkins**
Department of Aerospace Engineering
Auburn University

**Dr Donald J. Spring**
Department of Aerospace Engineering
Auburn University

**Mr Robert W. Bangert, Jr.**
SA-ALC/NW

**Mr Martin J. Cook**
Wright-Patterson AFB, Ohio

**Mr Newton England, Jr.**
SA-ALC/LCE

**Mr John R. Fenter**
WL/MT

**Mr Clark W. Furlong**
AFDTC/DRX

**Mr George F. Hepner**
Department of Geography
University of Utah

**Mr John J. Kaplan**
Albuquerque, New Mexico

**Mr Jack W. Lehner**
Vehicle Systems and Technology Office
Marshall Space Flight Center

**Mr Joseph J. Orlowski**
WL/XPR

**Mr David R. Selegan**
WL/CCI

## ALTERNATE FUTURES ASSESSORS

**Col Peter Engstrom, USAF, Retired**
Center for Information Strategy and Policy
Science Applications International Corporation

**Col Rolf Smith, USAF, Retired**
Office of Strategic Innovation

**Col Richard Wallace, USAF, Retired**
Center for Information Strategy and Policy
Science Applications International Corporation

**Dr Peter Bishop**
Associate Professor of Human Sciences
Chair of Graduate Programs and Studies of Futures
University of Houston, Clear Lake

**Mr Joe Haldeman**
Author
Professor, Massachusetts Institute of Technology

**Ms Christine A. R. MacNulty**
President
Applied Futures, Inc.

**Ms Christine McKeown**
Defense Intelligence Agency

**Mr Charles W. Thomas**
The Futures Group

**Mr Lee Vannes**
Booz, Allen & Hamilton

## STRATEGIC AIR WARFARE PANEL

**Dr James A. Mowbray, Director**
Chief
Air War College Faculty

**Maj Gen I. B. Holley, Jr., USAFR, Retired**
Department of History
Duke University

**Maj Gen William E. Jones, USAF, Retired**
Lockheed Martin Corporation

**Maj Gen Charles D. Link**
HQ USAF/AXO

**Air Vice-Marshal Richard A. Mason, RAF, Retired**
Foundation for International Security
United Kingdom

**Col Stephan Eisen, Jr.**
Air War College Faculty

**Gp Capt John P. Harvey**
Air Power Studies Centre
RAAF
Australia

**Gp Capt Anthony P. N. Lambert**
RAF Staff College
United Kingdom

**Lt Col Patrice Claveau**
EMAA-BPG

**Lt Col Bernhard G. Fuerst**
Fachbereich Fuehrungslehre
Luftwaffe

**Lt Col Marc Oellet**
Canadian Air Force

**Lt Col Barry Watts, USAF, Retired**
Northrop-Grumman Corporation

**Lt Col Axel E. Wilcke**
Fachbereich Fuehrungslehre
Luftwaffe

**Dr Stephen J. Cimbala**
Pennsylvania State University

**Dr Richard L. DiNardo**
Assistant Professor of History
Saint Peter's College

**Dr Alan W. Stephens**
Air Power Studies Centre
RAAF
Australia

**Mr Carl H. Builder**
RAND